

(19)



JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: 10200530 A

(43) Date of publication of application: 31 . 07 . 98

(51) Int. Cl.

H04L 12/24
H04L 12/26
G06F 13/00
H04L 12/46
H04L 12/28

(21) Application number: 09334093

(22) Date of filing: 04 . 12 . 97

(30) Priority: 23 . 12 . 96 US 96 773542

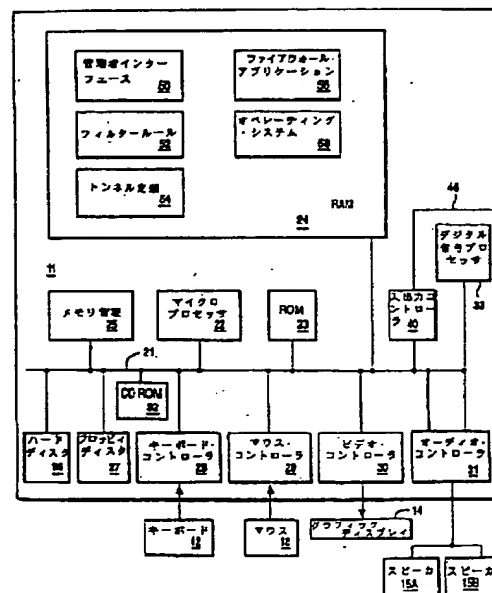
(71) Applicant: INTERNATL BUSINESS MACH
CORP <IBM>(72) Inventor: THEODORE JACK LONDON
SCHRADER(54) MANAGEMENT METHOD AND SYSTEM
THEREFOR

(57) Abstract:

PROBLEM TO BE SOLVED: To obtain a user-friendly interface for an internet protocol tunneling management of an internet fire wall by performing tunneling management of a fire wall computer between secure computer networks and computer networks that are not secure.

SOLUTION: A system unit 11 shows a graphic chart of tunnels among addresses of plural networks as lines that connect icons, which show network addresses on a display 14. The definition of a selection tunnel that is shown by a 1st line, according to the selection of a user of the 1st line, is shown in another partition of an interface. At this time, the action to selection tunnel definition is available according to the input of the user. A graphic chart of tunnels is selectively changed by the user's input, and all the defined tunnels, etc., can be shown.

COPYRIGHT: (C)1998,JPO



(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平10-200530

(43) 公開日 平成10年(1998) 7月31日

(51) Int. Cl. ⁸	識別記号	F I	
H 0 4 L 12/24		H 0 4 L 11/08	
12/26		G 0 6 F 13/00	3 5 5
G 0 6 F 13/00	3 5 5	H 0 4 L 11/00	3 1 0 C
H 0 4 L 12/46			
12/28			

審査請求 未請求 請求項の数22 O L (全 35 頁)

(21) 出願番号 特願平9-334093

(22) 出願日 平成9年(1997)12月4日

(31) 優先権主張番号 08/773542

(32) 優先日 1996年12月23日

(33) 優先権主張国 米国 (US)

(71) 出願人 390009531

インターナショナル・ビジネス・マシーンズ・コーポレーション

INTERNATIONAL BUSINESS MACHINES CORPORATION

アメリカ合衆国10504、ニューヨーク州

アーモンク (番地なし)

(72) 発明者 セオドア・ジャック・ロンドン・シュレイダー

アメリカ合衆国78613、テキサス州、セダー・パーク、シャディー・ブルック・レイ 1704

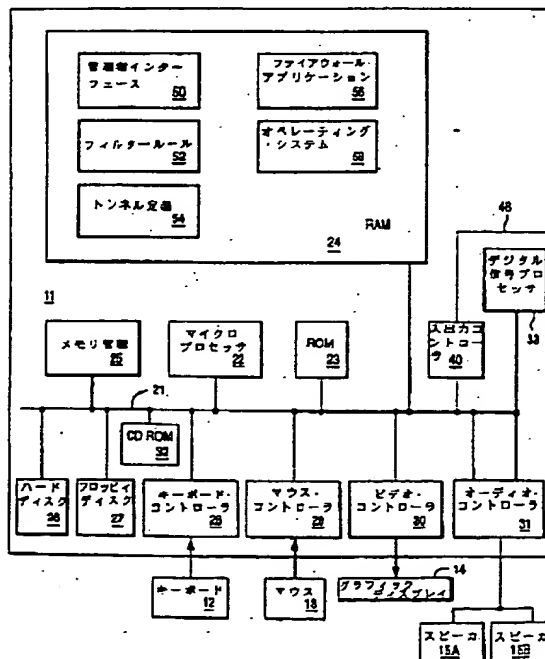
(74) 代理人 弁理士 坂口 博 (外1名)

(54) 【発明の名称】 管理方法およびシステム

(57) 【要約】

【課題】 ウェブ・ベースのインターフェースで安全なコンピュータ・ネットワークと安全でないコンピュータ・ネットワーク間のファイアウォール・コンピュータのトンネリングの管理を提供すること。

【解決手段】 複数のネットワークのアドレス間のトンネルのグラフィック図がネットワーク・アドレスを示すアイコンを接続するラインとして表示される。第一ラインのユーザの選択に応じて、第一ラインによって示された選択トンネルの定義がインターフェースの別の区画(ペイン)に表示される。この時点で、選択トンネル定義へのアクションはユーザ入力に応じて行うことが可能である。トンネルのグラフィック図はユーザの入力により選択的に切り換えられ、全ての定義されたトンネルや、活動中のトンネルや、活動していないトンネル等を示すことができる。照会が入力トンネル定義について実行されて、既存のトンネル定義が入力トンネル定義と照合するかどうか判定する。



【特許請求の範囲】

【請求項1】安全なコンピュータ・ネットワークと安全でないコンピュータ・ネットワーク間のファイアウォール・コンピュータにおけるトンネリングを管理する方法において、複数のネットワークのアドレス間のトンネルのグラフィック図をネットワーク・アドレスを示すアイコンを接続するラインとして表示するステップと、第一ラインのユーザの選択に応じて、その第一ラインによって示された選択したトンネル定義を表示するステップと、ユーザ入力に応じて、上記選択したトンネル定義へのアクションを行うステップとを有することを特徴とするファイアウォール・コンピュータのトンネリングを管理する方法。

【請求項2】上記トンネルのグラフィック図は、ユーザ入力により、全ての定義したトンネルを示し、活動中のトンネルを示し、あるいは非活動中のトンネルを示すように選択的に変えることが可能であることを特徴とする、請求項1に記載の方法。

【請求項3】上記ラインは、各々のトンネルの特性を示す異なった方法で描かれていることを特徴とする、請求項1に記載の方法。

【請求項4】上記特性はトンネルに可能な安全状態であることを特徴とする、請求項3に記載の方法。

【請求項5】上記グラフィック図は各トンネルが発生してくる方向を示す印を有することを特徴とする、請求項1に記載の方法。

【請求項6】安全なコンピュータ・ネットワークと安全でないコンピュータ・ネットワーク間のコンピュータのトンネリングを管理する方法において、トンネル定義を入れることのできる第一区画を有するユーザ・インターフェースを示すステップと、ユーザ入力に応じて、入力されたトンネル定義と既存のトンネル定義が照合するか判定するために、入力されたトンネル定義についての照会を実行するステップと、上記照会の結果を分散バーでユーザ・インターフェースの別な区画に表示し、トンネル定義の照合の位置は分散バーを通るラインにより示されるステップと、ユーザ入力に応じて、選択トンネル定義についてのアクションを行うステップとを有することを特徴とするコンピュータのトンネリングを管理する方法。

【請求項7】第三区画でトンネル定義のリストを表示し、そこでは照合するトンネル定義が照合しないトンネル定義とは異なった方法で表示するステップと、上記分散バーに隣接し、上記分散バーによって示されたトンネル定義の完全なリストに関して第三区画に表示したトンネル定義のリストの位置を示す小さなバーを表示するステップとを、さらに有することを特徴とする請求項6に記載の方法。

【請求項8】上記分散バーに隣接し、照合するトンネル定義の集中を示す小さなバーを表示するステップを、さ

らに有することを特徴とする請求項6に記載の方法。

【請求項9】安全なコンピュータ・ネットワークと安全でないコンピュータ・ネットワーク間のファイアウォール・コンピュータのトンネリングを管理する方法において、

複数のネットワークのアドレス間のトンネルのグラフィック図をネットワーク・アドレスを示すアイコンを接続するラインとして表示するステップと、

第一ラインのユーザの選択に応じて、その第一ラインによって示された選択したトンネルに適用できるフィルタ・ルールをリストを表示するステップと、

ユーザ入力に応じて、上記選択したフィルタ・ルールへのアクションを行うステップとを有することを特徴とするファイアウォール・コンピュータのトンネリングを管理する方法。

【請求項10】ユーザ入力に応じて、選択したトンネルに既存のフィルタ・ルールが応用可能か判定するために、選択したトンネルについての照会を実行するステップと、

上記照会の結果を分散バーでユーザ・インターフェースの別な区画に表示し、フィルタ・ルールの照合の位置は分散バーを通るラインにより示されるステップとを更に有することを特徴とする、請求項9に記載の方法。

【請求項11】照合するフィルタ・ルールを、フィルタ・ルールのリストの照合しないフィルタ・ルールとは異なった方法で表示するステップと、

上記分散バーに隣接し、上記分散バーによって示されたフィルタ・ルールの完全なリストに関して第三区画に表示したフィルタ・ルールのリストの位置を示す小さなバーを表示するステップとを、さらに有することを特徴とする請求項10に記載の方法。

【請求項12】安全なコンピュータ・ネットワークと安全でないコンピュータ・ネットワーク間のファイアウォール・コンピュータのトンネリングを管理するためのプロセッサとメモリを有するシステムにおいて、

複数のネットワークのアドレス間のトンネルのグラフィック図をネットワーク・アドレスを示すアイコンを接続するラインとして表示する手段と、

第一ラインのユーザの選択に応じて、その第一ラインによって示された選択したトンネル定義を表示する手段と、

ユーザ入力に応じて、上記選択したトンネル定義へのアクションを行う手段とを有することを特徴とするファイアウォール・コンピュータのトンネリングを管理するシステム。

【請求項13】上記トンネルのグラフィック図は、ユーザ入力により、全ての定義したトンネルを示し、活動中のトンネルを示し、あるいは非活動中のトンネルを示すように選択的に変えることが可能であることを特徴とする、請求項12に記載のシステム。

【請求項14】上記ラインは、各々のトンネルの特性を示す異なった方法で描かれていることを特徴とする、請求項12に記載のシステム。

【請求項15】上記特性はトンネルに可能な安全状態であることを特徴とする、請求項14に記載のシステム。

【請求項16】上記グラフィック図は各トンネルが発生してくる方向を示す印を有することを特徴とする、請求項12に記載のシステム。

【請求項17】安全なコンピュータ・ネットワークと安全でないコンピュータ・ネットワーク間のファイアウォール・コンピュータのトンネリングを管理するためのプロセッサとメモリを有するシステムにおいて、

トンネル定義を入力することのできる第一区画を有するユーザ・インターフェースを示す手段と、

ユーザ入力に応じて、入力されたトンネル定義と既存のトンネル定義が照合するか判定するために、入力されたトンネル定義についての照会を実行する手段と、

上記照会の結果を分散バーでユーザ・インターフェースの別な区画に表示し、トンネル定義の照合の位置は分散バーを通るラインにより示される手段と、

ユーザ入力に応じて、選択トンネル定義についてのアクションを行う手段とを有することを特徴とするファイアウォール・コンピュータのトンネリングを管理するシステム。

【請求項18】第三区画でトンネル定義のリストを表示し、そこでは照合するトンネル定義が照合しないトンネル定義とは異なった方法で表示する手段と、

上記分散バーに隣接し、上記分散バーによって示されたトンネル定義の完全なリストに関して第三区画に表示したトンネル定義のリストの位置を示す小さなバーを表示する手段とを、さらに有することを特徴とする請求項17に記載のシステム。

【請求項19】上記分散バーに隣接し、照合するトンネル定義の集中を示す小さなバーを表示する手段を、さらに有することを特徴とする請求項17に記載のシステム。

【請求項20】安全なコンピュータ・ネットワークと安全でないコンピュータ・ネットワーク間のファイアウォール・コンピュータのトンネリングを管理するプロセッサとメモリを有するシステムにおいて、

複数のネットワークのアドレス間のトンネルのグラフィック図をネットワーク・アドレスを示すアイコンを接続するラインとして表示する手段と、

第一ラインのユーザの選択に応じて、その第一ラインによって示された選択したトンネルに応用できるフィルタ・ルールのリストを表示する手段と、

ユーザ入力に応じて、上記選択したフィルタ・ルールへのアクションを行う手段とを有することを特徴とするファイアウォール・コンピュータのトンネリングを管理するシステム。

【請求項21】ユーザ入力に応じて、選択したトンネルに既存のフィルタ・ルールが応用可能か判定するために、選択したトンネルについての照会を実行する手段と、

上記照会の結果を分散バーでユーザ・インターフェースの別な区画に表示し、フィルタ・ルールの照合の位置は分散バーを通るラインにより示される手段とを更に有することを特徴とする、請求項20に記載の方法。

【請求項22】照合するフィルタ・ルールを、フィルタ・ルールのリストの照合しないフィルタ・ルールとは異なった方法で表示する手段と、

上記分散バーに隣接し、上記分散バーによって示されたフィルタ・ルールの完全なリストに関して第三区画に表示したフィルタ・ルールのリストの位置を示す小さなバーを表示する手段とを、さらに有することを特徴とする請求項21に記載の方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は分散型コンピュータ・ネットワークの安全システムに関する。特に、安全でないインターネットと安全な企業内ネット間に見られるようなコンピュータのIPトンネリングを管理するためのウェブ・ベースのインターフェースに関する。

【0002】本出願は、共通の譲渡人による米国特許出願である1996年12月23日出願、出願番号773543、発明者T. Shrad erによる「インターネット・ファイアウォールのIPフィルタ処理のウェブ・ベースの管理」に関連した発明である。

【0003】

【従来の技術】インターネット管理者の負担は急速に量や複雑さが増大してきた。企業あるいは組織の安全な内部ネットを外部の安全ではないインターネットに接続するインターネット・ファイアウォールを管理するために複数の管理者と協力する、管理責任者が必要である。従来技術では一般に、ファイアウォールのインターフェースは管理者がインターネット・ファイアウォール特性とオペレーションを管理する事を可能にするコマンド・ラインあるいはSMITインターフェースである。これらのタイプのインターフェースは多くのコマンドの記憶化を要求し、また、管理者はファイアウォールを支配するトンネル・ルールを管理するために異なったアクションからの出力を継ぎ合わせる必要がある。これは管理者が複数のスクリーンからの情報を記憶したり、ライトダウンしなければならない時に、明らかに不便である。つまり、従来のインターフェースは決してユーザにとって扱い易いわけではない。

【0004】

【発明が解決しようとする課題】本発明はインターネット・ファイアウォールのIPトンネリングの管理のためにユーザが使い易いインターフェースを提供することを目

10

20

30

40

50

的とする。

【0005】さらに、本発明の目的はファイアウォール・コンピュータのIPトンネリングを管理するためのインターフェースを改良することである。

【0006】

【課題を解決するための手段】上記目的は、安全なコンピュータ・ネットワークと安全でないコンピュータ・ネットワーク間のファイアウォール・コンピュータのトンネリングを管理することにより達成される。

【0007】望ましい一実施例では、複数のネットワークのアドレス間のトンネルのグラフィック図がネットワーク・アドレスを示すアイコンを接続するラインとして表示される。第一ラインのユーザの選択に応じて、第一ラインによって示された選択トンネルの定義がインターフェースの別の区画（ペイン）に表示される。この時点で、選択トンネル定義へのアクションはユーザ入力に応じて行うことが可能である。トンネルのグラフィック図はユーザの入力により選択的に切り換えられ、全ての定義されたトンネルや、活動中のトンネルや、活動していないトンネル等を示すことができる。

【0008】本発明の別の実施例では、ユーザ・インターフェースは一つのトンネル定義を入れることのできる第一区画を持つように提供される。照会が入力トンネル定義について実行されて、既存のトンネル定義が入力トンネル定義と照合するかどうか判定する。この照会の結果がユーザ・インターフェースの別の区画に分散バーで表示され、照会したトンネル定義の位置をその分散バーを通ったラインにより示される。小さなバーが分散バーの近くで表示され、その小さなバーは分散バーにより示されたトンネル定義の全リストに関係のあるトンネル定義の表示リストの位置を示している。この時点で、一つの選択したトンネル定義についてアクションが行える。

【0009】本発明のさらに別な実施例では、ネットワークにおけるアドレス間のトンネルのグラフィック図が、ネットワーク・アドレスを示すアイコンに接続するラインとして提供される。第一ラインのユーザの選択に応じ、第一ラインにより示された選択トンネルに適用可能なフィルタ・ルール・リストが表示される。分散バーはユーザ・インターフェースの別の区画に表示される。そこで、分散バーにより示される全てのフィルタ・ルール・リスト内で、フィルタ・ルールと照合する位置が分散バーを通るラインにより示される。この時点で、ユーザ入力に応じ、選択したフィルタ・ルールについてアクションを行うことができる。

【0010】

【発明の実施の形態】本発明は複数の異なったオペレーティング・システム下にある種々のコンピュータあるいは複数のコンピュータの集まりで実行できる。例えば、コンピュータはパーソナル・コンピュータ、ミニ・コンピュータ、メインフレーム・コンピュータ、あるいは他

のコンピュータの分散ネットワークで実行するコンピュータ等である。コンピュータの選択はプロセッサ速度やディスク記憶の要求などによってのみ制限されるが、IBM PCシリーズのコンピュータは本発明に使用可能である。IBMパーソナル・コンピュータが実行できるオペレーティング・システムの一つはIBMのOS/2 Warp 4.0である。別に、コンピュータ・システムがAIX（登録商標）オペレーティング・システムで実行するコンピュータのIBM RISCシステム/6000（登録商標）ラインにある。

【0011】図1では、システム・ユニット11、キーボード12、マウス13、ディスプレイ14を有するコンピュータがブロック図で示されている。システム・ユニット11は、種々の構成部品が接続されている単独のシステム・バス、あるいは複数のシステム・バス21を有し、それにより種々の構成部品間で通信が行われる。マイクロプロセッサ22はシステム・バス21に接続され、またシステム・バス21に接続されている読取り専用メモリ（ROM）23とランダム・アクセス・メモリ（RAM）24によりサポートされている。IBM PCシリーズのコンピュータのマイクロプロセッサはIntel 1386、486あるいはPentiumマイクロプロセッサ等の一種である。しかし、Motorola社の68000、68020、68030等のマイクロプロセッサも、特に限定されないが使用でき、またIBM社のPower PCチップのような縮小命令セット・コンピュータ（RISC）も含まれる。Hewlett Packard、Sun、Motorola社等により作られた他のRISCチップもこのコンピュータに使用可能である。

【0012】ROM 23は、特に、対話およびディスク・ドライブ、キーボードのような基本的なハードウェア・オペレーションを制御するBIOS（基本動作命令プログラム群）を含む。RAM 24は、オペレーティング・システムやアプリケーション・プログラムをロードされている主メモリである。メモリ管理チップ25はシステム・バス21に接続されており、RAM 24とハード・ディスク・ドライブ26およびフロッピー・ディスク・ドライブ27間のデータを含み、通過させる直接メモリ・アクセス・オペレーションを制御する。システム・バス21に接続したCD-ROM 32も、例えばマルチメディア・プログラムや図形表示のような多量のデータを記憶するために使われる。

【0013】また、このシステム・バス21に種々の入力/出力コントローラを接続しており、例えばキーボード・コントローラ28、マウス・コントローラ29、ビデオ・コントローラ30、オーディオ・コントローラ31などである。既知のごとく、キーボード・コントローラ28はキーボード12のハードウェア・インターフェースを提供し、マウス・コントローラ29はマウス13のハードウェア・インターフェースを提供し、ビデオ・コントローラ30はディスプレイ14のハードウェア・

インターフェースであり、オーディオ・コントローラ31はスピーカ15のハードウェア・インターフェースである。トークン・リング・アダプタのような入力/出力コントローラ40は、ネットワーク46を通じて、同様に構成された他のデータ処理システムとの通信を可能とする。

【0014】本発明の望ましい実行例の一つは、上記したように構成した1つ以上のコンピュータ・システムのRAM24にある複数の命令50-58のセットである。コンピュータ・システムが要求するまで、その命令セットは、例えば、ハード・ディスク・ドライブ26、あるいは取り出し可能なメモリ、つまりCD-ROM32で随時使用できる光ディスクや、フロッピー・ディスク・ドライブ27で随時使用できるフロッピー・ディスク等の、別のコンピュータで読取り可能なメモリに記憶させることができる。さらに、その命令セットは別のコンピュータのメモリに記憶させることが可能であり、またユーザの望みによりローカル・エリア・ネットワークやインターネットのようなワイド・エリア・ネットワークを通じて送信することができる。この命令セットの物理的な記憶は電氣的、磁氣的、あるいは化学的に記憶させた媒体を物理的に変更し、その媒体はコンピュータが読取り可能な情報を担持することは当業界では公知である。本発明を命令、記号、文字等について説明することは便利であるが、それらの全ておよび同様な用語は適切な有形の構成要素と関連させるべきである。

【0015】さらに、本発明は頻繁に比較あるいは確認すること、または人間のオペレータと組み合わせることが可能な表現で説明する。人間のオペレータによるアクションを行わないことが、本発明の一部を形成するオペレーションで望ましい。このオペレーションは他の電気信号を発生する電気信号を処理する機械操作である。

【0016】IBM社のSecure Way Firewall (SWF)のようなインターネットのファイアウォール製品は、インターネットの内部安全ネットワークと外部の安全でないネットワーク間の物理的なファイアウォールを管理者が作ることを可能とする。ファイアウォール装置の物理的な接続のほかにも、ファイアウォール製品は、安全なネットワークから出し入れする情報の流れを管理者が制御することを助ける複数の機能を提供する。そうした機能はテルネット (telnet)、FTP代理サービス、SOCKSサービス、特別のドメイン名サービス、安全なネットワーク間のインターネット中のIPトンネリング、IPパケットの安全なネットワークへの出入りを許可、あるいは拒絶の判定をするためのフィルタ・ルールの実行等である。

【0017】こうしたフィルタ・ルールの一つはIPの偽物に対する防護を行うことであり、そのIPの偽物とは、アタッカがあるIPパケットを変えて、そのアタッカのワークステーションと同じではないソースIPアド

レスから来たかのように見せようとするものである。管理者はIPフィルタを設定し、安全なネットワークに対し内部にあるが、安全ではないネットワークから来ているソースIPアドレスを有するIPパケットを拒絶する。

【0018】図2は2つのネットワークを利用するファイアウォール構成の一例を示す。ここでは、一つの装置100だけが防護拠点としてファイアウォールに含まれており、すべてのIPパケットはこの装置を介して安全でないネットワーク110から安全なネットワーク120へ、あるいはその逆へ送られる。このファイアウォール装置100は、ファイアウォールで実施可能あるいは実施不可能なアプリケーション・ゲートウェイに対するファイアウォールの置き換えに加えて設けられたスクリーニング・フィルタ、またはIPフィルタを有している。

【0019】図3はスクリーニング・フィルタを有する別の装置140の後ろに防護装置130を配置した、別の構成を示している。この構成は、IPパケットが防護装置のアプリケーション・ゲートウェイによって処理される前に、初めにファイアウォールを通して許可されなければならないので、さらにファイアウォールに対する防護を提供することになる。安全でないネットワークおよび安全なネットワークが、それぞれ150160に示されている。

【0020】IPトンネリングは、本発明の主題であるインターネット・ファイアウォールにより提供された機能である。管理者は、IPパケットが流れる2つのインターネット防護壁間のトンネルを定義することができる。管理者がIPトンネルをどのように定義したかに応じてファイアウォール間のインターネットを流れるIPパケットを符号化するのと同時に、このトンネルはソースと宛先アドレス間に立証を課す。

【0021】IPトンネルの全体的な説明は、バーチャル・プライベート・ネットワーク (VPN) のインターネット技術者のタスク・フォース (IETF) で与えられる。

【0022】ファイアウォールによって行うIPトンネリングやフィルタ処理のプロセスは公知技術では詳細な説明はされていない。さらに、それらはハードウェアに影響されるだけでなく、特別なファイアウォール技術により変化する。以下に説明するウェブ・ベースのインターフェースは、ユーザ入力に応じた必要な機能を行うためにAPIあるいは他のソフトウェア・インターフェースを介してファイアウォールを単に呼び出すだけである。これは実用的ではないが、ファイアウォールの機能はインターフェースを有するウェブ・ページに複製される。

【0023】ファイアウォール・コンピュータそのものに残らなくてはならない公知技術のインターフェースと

は逆に、本発明のウェブ・ベースのインターフェースは管理者のシステムとファイアウォール・システム間で求められる適切な安全性を有するネットワークのどのコンピュータにも残ることができる。インターフェースは安全なネットワーク内のファイアウォールあるいは別のシステムにあることが可能であるが、ファイアウォールの管理も特に信用のあるアドレスで安全なネットワークの外側で起こすことも可能である。しかし、これは安全の観点からあまり望ましいものではない。それにも拘わらず、このインターフェースは軽便であり、従来技術では不可能だった柔軟性を管理者に与えることができる。

【0024】上記説明のように、従来技術のインターフェースは通常、管理者が不可解な多数のコマンドを学習することを強いられたコマンド・ラインを基本としている。本発明はウェブ・ベースのユーザ・インターフェースのフレームワークを用いる。IPTunnelに対する管理者のタスクは、IPTunnelの定義、IPTunnelのグラフィックス表示、IPTunnelの照会、IPTunnelの定義を有するIPフィルタ・ルールの照会等に分けられる。望ましい一実施例では、ユーザ・インターフェースは次のウェブ・ページに分けられる。

【0025】＊IPTunnelの定義のページ

＊IPTunnelのグラフィックスのページ

＊IPTunnelの照会のページ

＊IPTunnel/フィルタの照会のページ

【0026】これらのページの詳細な説明をする。すなわち、本発明は、ウェブ・ベースの管理ブラウザの全ての機能のセットを管理者がインストール、あるいは使用する必要がないような設計モジュールである。管理者がフィルタ・ルールの管理にだけ関心があるなら、SOC KSサーバやIPTunnelingに対してのような、その他の管理機能に繋がるパスは引用する必要がない。他の機能は必要な時にプラグ・インさせることが可能である。

【0027】本発明は、従来技術のインターフェースでは有効ではなかったウェブ・ベースのファイアウォール・フレームワークへIPTunnelingに関する多くの機能を加え、同時にその低レベルのページの配置を矛盾無く維持する。このモジュール・レベルの各ページは複数の区画（あるいはフレーム）に分割され、各区画はページに関係なく特定のタイプの情報を表示する。従って、管理者は情報があるページに応じた情報の前後関係を予測することができる。

【0028】典型的なページのレイアウトを以下に説明する。図4にはIPTunnel定義ページが示されている。ナビゲーション区画200がこのページの最上部に示される。この区画により、管理者はテキストかアイコンを選択してファイアウォール・インターフェースの管理モジュールか他のモジュールの他の部分をナビゲートする。

【0029】ナビゲーション区画200の下には、ディスプレイ区画210とディスプレイ・アクション区画220が表示されている。ディスプレイ区画210はエントリ・フィールド212あるいはアクティブ・ファンクションの押しボタン214を示すページの場所を提供する。スクロール・バー216を別のエントリ・フィールド用に設ける。他の区画には、そのページの初めの情報のグラフィックス表示が示される。IPTunnelのグラフィックス・ページに対して、この区画は安全なネットワーク間の接続を絵画的に示すことになる。

【0030】ディスプレイ・アクション区画220は、管理者が押しボタン222によりディスプレイ区画のオブジェクトの定義を修正したり、保存することを開始可能なアクションを提供する。あるいは、管理者によって開始されたアクション（図示せず）の結果を示す。

【0031】このページの次のレベルはメータ区画230、リスト区画240、リスト・アクション区画250に分割されている。このレベルの主区画はリスト区画240であり、これは管理者が該当区画に属する全てのエントリを見ることを可能とする。IPTunnel定義のページについて、リスト区画が定義済みのIPTunnelのリスト242を管理者に示す。スクロール・バー244、246は別のエントリや複数のエントリについての情報を表示するためのオプション的な機能である。

【0032】リスト・アクション区画250は、ディスプレイ・アクション区画と同じように動作する。管理者は押しボタン252を作動させてリスト区画のエントリに関連するアクションのリストから、IPフィルタ・ルールの完全なリストを記憶、あるいは目標最終点のファイアウォールにIPTunnel定義のリストを送ること等を選択できる。

【0033】メータ区画230は、表示区画により開始させられた統計、あるいはリスト区画内の全統計に関する情報を画像的あるいは文章的表现で表示する。トンネル定義ページにおいて、トレースルート、ビーンという音、指によるルーチンの出力が表示される。

【0034】チック・テープ区画260はこのページの一番下にあり、このページのエントリやオブジェクトについての動的情報や統計の情報を管理者に提供する。情報は右から左にスクロールし、管理者がこのページでアクションを開始する際に更新される。

【0035】望ましい実施例では、ウェブ・ベースの管理ページは、Netscape Navigator（登録商標）ブラウザのような、htmlやJava（登録商標）アプレットを支援するウェブ・ブラウザにおいて使用できる。図から明らかなように、全てのウェブ・ページは管理者に対して矛盾のない使い易いレイアウトを提供する。

【0036】IPTunnel定義ページを詳細に説明する。IPTunnel定義ページは管理者が次のアクションを行うことを可能にする。

* あるファイアウォールについて記憶したIPトンネル定義を見る。

* 新しいIPトンネル定義を作る。

* 記憶したIPトンネル定義を修正する。

* IPトンネル定義をロードあるいは保存する。

* 記憶したIPトンネル定義を配布する。

* 記憶したIPトンネル定義を活性化あるいは不活性化する。

* IPトンネル定義を停止する。

* 2つのファイアウォール間でIPトンネル定義を確認する。

【0037】管理者はディスプレイ区画210のエントリ・フィールド212やリスト・ボックス214、およびディスプレイ・アクション区画222の押しボタン222アクションを使ってIPトンネル定義を作成したり、修正したりできる。リスト区画240はインターネット・ファイアウォール用に定義された全てのIPトンネル定義を表示する。管理者はそれらをスクロールし、修正または削除用のIPトンネル定義を明るく点灯させ、リスト・アクション区画250の押しボタン252により一つのアクションを選択して、ファイアウォールに送る等のIPトンネル定義についてのオペレーションを行う。

【0038】ウェブ管理ブラウザが実行されるホストの目標IPアドレスに管理者がアクセス可能なら、その管理者はエントリ・フィールドに隣接した適切なボタンを押すことにより、目標IPアドレスをピンと鳴らす、トレースルートする、指で指示することが可能である。例えば、管理者はソース・アドレスに隣接したピン・ボタンを押すと、インターフェースはソース・アドレス・フィールドのピン・プロセスを実行する。これらのアクションの出力はメータ区画230に現れる。および別の方法でテーブル区画260をチャック作動する。この機能は、管理者がインターフェースから離れる必要なくIPアドレスが到達可能、あるいは識別可能か容易に判定する。チャック・テーブル区画もIPトンネル定義についての統計的情報、つまり同じソースと宛先アドレス間で定義されたトンネルの数等の情報をピン機能あるいは指機能の出力を表示するために使われてない時に、表示する。

【0039】ここでは、この図に示されているインターフェースから始めることができるシステム・アクションの全てが説明されている訳ではなく、このウェブ・ページで実行可能なアクションの説明である。

【0040】図5のIPトンネル画像ページは、2つのインターネット・ファイアウォール間で定義されたIPトンネルを管理者が画像的に見ることを可能にする。このウェブ・ページは、左側のファイアウォールのソース・アドレスを表すボックス313と右側の目標ファイアウォールの宛先アドレスを表すボックス314、315、316を有するディスプレイ区画310に画像31

2を示している。IPトンネルが2つのアドレス間で定義されている場所で、このウェブ・ページは2つのボックス間にライン317を引き、そのラインにシンボル318を付けてどのアドレスがそのトンネルを開始するか、およびそのIPトンネルのIDを示す。このラインは異なった種類を使用して引かれ、安全状態のような特性を示す。つまり、このトンネルが符号化あるいは認可可能であるか、あるいはその組合せが可能であるかどうか示す。ディスプレイ・アクション区画320は、管理者がボタン322、324、326を押すことにより、定義されたIPトンネル定義の全て、ファイアウォールで活動中のものだけ、あるいはファイアウォールで活動中ではないものだけを見ることを可能とする。

【0041】メータ区画330はディスプレイ区画のIPトンネル・ラインの説明333を表示する。望ましい一実施例では、この区画は同様に他の動的情報も表示する。

【0042】リスト区画は、このファイアウォールについて定義したIPトンネル定義の全てのスクロール可能なリスト342を表示することになる。管理者はこのディスプレイ区画310のIPトンネル・ラインを選択して点灯したウェブ・ページを有し、またリスト区画340内に全てのトンネル定義342を示す。リスト・アクション区画350の押しボタン352により管理者は、あるファイアウォールについての選択したIPトンネル定義を活性化したり、不活性化したり、編集したり、削除したりすることに加え、IPトンネル定義のリストをロードあるいは保存することが可能である。

【0043】この図に示されているアクションの全てが説明されている訳ではなく、このウェブ・ページで実行可能なアクションの説明である。

【0044】図6はIPトンネル照会ページを示しており、記憶したIPトンネル定義集合に対して管理者が照会を実行してその照会と照合する全ての定義を見ることができる。照会も複数のワイルドカードをサポートする。例えば、ある宛先への照会で特定した基準と照合した、あるIPトンネル定義をリターンさせるワイルドカードで、宛先アドレスを特定することができる。

【0045】管理者は照会ページのディスプレイ区画410で照会を定義することができる。トンネルIDのエントリ・フィールド、ソース・アドレス、宛先アドレス、符号化アルゴリズム、符号化ポリシー等が設けられている。望ましい一実施例では、以前の照会は新たな照会のモデルとして、あるいは修正せずに再度実行させるために、保存、検索、表示等ができる。反復の実行が考えられる照会を保存することは利点が多い。このリストのIPトンネル値から誘導した選択リストは、IPトンネルのリストのIDとアドレスのセットからIPトンネルIDまたはアドレスのリストを提供する。

【0046】図に示したように、ディスプレイ・アクシ

ョン区画420は、ディスプレイ区画をクリアする押しボタン422とディスプレイ区画で定義した照会の実行424の2つのアクションを管理者に提供する。このディスプレイ・アクション区画420も、照会テストと照合したIPトンネル定義の数を示す大きな字体の数字426を表示する。

【0047】メータ区画430は照合したIPトンネル定義の分布を視覚的に示すグラフィカル・バー432を表示する。これらの照合したIPトンネル定義はバーの他の部分とは異なる色を着けられている。このバー432は、視覚的かつ迅速に照合したIPトンネル定義およびIPトンネル定義リスト内の分布を示すので分散バーと呼ばれる。この分散バー432に隣接した小さなバー434が位置的なキューとして使われ、リスト区画440内に現在表示されているIPトンネル定義を示す。その小さいバー434あるいは第二の小さなバーも、照合した、またはほぼ照合しているトンネル定義が見つかるリスト内のエリアを示すために使用できる。

【0048】リスト区画440は、ファイアウォールに対して定義した全てのIPトンネル定義のスクロール可能なリスト442を表示する。照合したIPトンネル定義は異なった色、または明るく点灯して表示される。管理者はエントリを選択して（または明るく点灯させて）それを編集したり、あるいはIPトンネル定義リストから削除する。読みやすくするため、IPトンネル・エントリを縦列に分割し、全てのソース・アドレスが水平方向に並べられる。

【0049】リスト・アクション区画450は、押しボタン452を作動させることにより管理者は、あるファイアウォールについての選択したIPトンネル定義のリストをロードすることが可能である。また、エントリ編集の押しボタン454を作動させることにより選択したIPトンネル定義を編集することが可能である。エントリ編集の押しボタン454を作動させることにより、IPトンネル定義ページに表示した選択エントリの定義を有するIPトンネル定義ページに管理者を戻す。

【0050】図7はIPトンネル/フィルタ照会ページを示す表示例である。このページは、あるインターネット。ファイアウォールについての2つの別な定義グループである、IPトンネル定義およびIPフィルタ定義をまとめたものである。このIPフィルタ・グループは冒頭に明示した出願書類に説明されている。IPトンネル画像ページに示したのと同じIPトンネル画像の選択に基づくIPフィルタ・ルールのリストに対して照会を管理者が行うことを可能とする。この画像512はディスプレイ区画510に示されている。画像のIPトンネル・ライン514およびディスプレイ・アクション区画の照会実行ボタン524を選択することは、ファイアウォール・フィルタ・ルールのリストにある照会を起こすことになる。IPフィルタ・ルールはIPトンネル情報を

含む必要がないが、管理者は、例えば、符号化を用いて定義したIPトンネルを通じて、特定のソース・アドレス、宛先アドレス、ポート番号から全てのIPパケットの経路を定めるための受け入れフィルタ・ルールを定義することができる。

【0051】ディスプレイ・アクション区画520は管理者に2つのアクションの選択を提供する。すなわち、一方のボタン522はディスプレイ区画の明るく点灯しているIPトンネル選択をクリアし、もう一方のボタン524は選択したIPトンネル・ラインに基づくディスプレイ区画内で定義した照会を実行するためのものである。ディスプレイ・アクション区画もその選択したIPトンネルのID526、および照会テストで照合したIPフィルタ・ルールの番号を大きな字体で示す番号528を表示する。

【0052】IPトンネル照会ページでのように、メータ区画530はグラフィカル・バー532を表示するが、この場合には照合したIPフィルタ・ルールの分布を視覚的に示す。これらの照合したIPフィルタ・ルールはバーの他の部分とは異なる色で示される。このバー532は、視覚的かつ迅速に照合したIPフィルタ・ルールおよびIPフィルタ・ルール・リスト内の分布を示すので分散バーと呼ばれる。この分散バー532に隣接した小さなバー534が位置的キューとして使われ、リスト区画540内に現在表示されているIPフィルタ・ルールを示す。

【0053】リスト区画540は、ファイアウォールに対して定義した全てのIPフィルタ・ルールのリスト542を表示する。管理者がIPトンネル定義を表すディスプレイ区画510内のライン514を選択すると、このウェブ・ページは、同じIPトンネルIDで定義されたリスト542内のIPフィルタ・ルール全てに色を着ける。照合したIPフィルタ・ルールは明るく点灯しているエントリとは逆に、異なった色で表示するのが望ましい。というのは、明るく点灯しているものはインターフェース内の選択用に使われるからである。管理者はこのリスト内のエントリを選択し、フィルタ・リストから編集することができる。

【0054】リスト・アクション区画550は、フィルタ・リストのロードと示された押しボタン552を作動させることにより、管理者は、あるファイアウォールについてのIPフィルタ・ルールのリストをロードすることが可能である。また、編集エントリ押しボタン554を作動させることにより選択したIPフィルタ・ルールを編集することが可能である。フィルタ・ルールの編集については、フィルタ定義ページで引用した出願に説明されている。

【0055】IPトンネル・ページのデータ構造

【0056】IPトンネル・テーブル構造

IPトンネル構造の数

IPトンネル構造に対するポインタ

【0057】IPトンネル構造

トンネルID

目標アドレス

ローカル・アドレス

符号化アルゴリズム

セッション・キー寿命

セッション・キー再生時間

開始プログラム

立証ポリシー

符号化ポリシー

<他の変数も各について作成可能>

コメント

【0058】IPトンネル定義ページのデータ構造

修正したリスト区画の状態ビット

リスト区画のIPトンネル・テーブル構造

修正したディスプレイ区画の状態ビット

ディスプレイ区画のIPトンネル構造

【0059】IPトンネル画像ページのデータ構造

ディスプレイ区画のIPトンネル・テーブル構造

リスト区画IPのトンネル・テーブル構造

一時IPトンネル構造

【0060】IPトンネル照会ページのデータ構造

ディスプレイ区画のIPトンネル構造

ディスプレイ・アクション区画の照合トンネル数

メータ区画の上部区域

メータ区画の照合IPトンネル・テーブル

リスト区画のIPトンネル・テーブル構造

一時IPトンネル構造

【0061】IPトンネル/フィルタ照会ページのデータ構造

ディスプレイ区画のIPトンネル・テーブル構造

ディスプレイ・アクション区画の照合フィルタ数

メータ区画の上部区域

メータ区画の照合フィルタ・ルール・テーブル構造

リスト区画のフィルタ・ルール・テーブル構造

一時フィルタ・ルール構造

【0062】上記のデータ構造はIPトンネル・テーブル構造を含んでいる。この構造はファイアウォールについて定義した全てのIPトンネルを保有する。IPトンネル構造は単一のトンネル定義の全ての属性を表す。例えば、トンネル定義でのローカルおよび目標アドレスは、IPトンネルの終点のソース装置および宛先ファイアウォール装置を確立するため使用される。別のIPトンネル属性は、そのIPトンネルを通るIPパケット用に確立された符号化アルゴリズムおよび立証ポリシーの種類を含む。

【0063】IPトンネル定義ページのデータ構造は、このページで情報のトラックを表示したり保存するために使用されたデータ構造を含む。修正したリスト区画の

40

50

状態ビットは、トンネル定義が過去にこのインターフェースにロードされたのでIPトンネルのリストにトンネル定義が加えられたかどうかを示す。リスト区画のIPトンネル・テーブル構造はそのファイアウォールからロードされたトンネル定義の集合である。修正したディスプレイ区画の状態ビットは、管理者がそのディスプレイ区画で何らかの情報を変更したかどうかを示す。ディスプレイ区画のIPトンネル構造はディスプレイ区画そのものに示された全ての値を保持する。

10

【0064】IPトンネル画像ページのデータ構造は、このページの情報のトラックを表示したり保持したりするため使用したデータ構造を含む。ディスプレイ区画のIPトンネル・テーブル構造はファイアウォールからロードしたトンネル定義の集合であり、この情報はこのページでトンネルを画像表示するため使用している。リスト区画IPのトンネル・テーブル構造はファイアウォールからロードしたトンネル定義の集合である。一時IPトンネル構造は、このページで管理者のアクションの結果として情報がIPトンネル定義ページに伝送される時に使用される選択IPトンネル定義を保持するため使用されるものである。

20

【0065】IPトンネル照会ページのデータ構造は、このページで情報のトラックを表示したり保存するために使用されたデータ構造を含む。ディスプレイ区画のIPトンネル構造はディスプレイ区画そのものに表示した全ての値を保持する。ディスプレイ・アクション区画の照合トンネル数は、ディスプレイ区画でIPトンネルの照会明細と照合するインターフェースでロードされたトンネル定義の数である。メータ区画の上部区域はインターフェースでロードされたトンネル定義の数である。メータ区画の照合IPトンネル・テーブルはディスプレイ区画でIPトンネルの照会明細と照合するインターフェースでロードされたトンネル定義の集合である。リスト区画のIPトンネル・テーブル構造はファイアウォールからロードされたトンネル定義の集合である。一時IPトンネル構造は、このページで管理者のアクションの結果として情報がIPトンネル定義ページに伝送される時に使用される選択IPトンネル定義を保持するため使用されるものである。

40

【0066】IPトンネル/フィルタ照会ページのデータ構造は、このページで情報のトラックを表示したり保存するために使用されたデータ構造を含む。ディスプレイ区画のIPトンネル・テーブル構造は、ファイアウォールからロードしたトンネル定義の集合であり、この情報はこのページでトンネルを画像表示するため使用している。ディスプレイ・アクション区画の照合フィルタ数は、ディスプレイ区画で選択されたIPトンネルIDと照合するインターフェースでロードしたIPフィルタ・ルールの数である。メータ区画の上部区域はインターフェースでロードされたフィルタ・ルールの数である。メ

50

状態ビットは、トンネル定義が過去にこのインターフェースにロードされたのでIPトンネルのリストにトンネル定義が加えられたかどうかを示す。リスト区画のIPトンネル・テーブル構造はそのファイアウォールからロードされたトンネル定義の集合である。修正したディスプレイ区画の状態ビットは、管理者がそのディスプレイ区画で何らかの情報を変更したかどうかを示す。ディスプレイ区画のIPトンネル構造はディスプレイ区画そのものに示された全ての値を保持する。

10

【0064】IPトンネル画像ページのデータ構造は、このページの情報のトラックを表示したり保持したりするため使用したデータ構造を含む。ディスプレイ区画のIPトンネル・テーブル構造はファイアウォールからロードしたトンネル定義の集合であり、この情報はこのページでトンネルを画像表示するため使用している。リスト区画IPのトンネル・テーブル構造はファイアウォールからロードしたトンネル定義の集合である。一時IPトンネル構造は、このページで管理者のアクションの結果として情報がIPトンネル定義ページに伝送される時に使用される選択IPトンネル定義を保持するため使用されるものである。

20

【0065】IPトンネル照会ページのデータ構造は、このページで情報のトラックを表示したり保存するために使用されたデータ構造を含む。ディスプレイ区画のIPトンネル構造はディスプレイ区画そのものに表示した全ての値を保持する。ディスプレイ・アクション区画の照合トンネル数は、ディスプレイ区画でIPトンネルの照会明細と照合するインターフェースでロードされたトンネル定義の数である。メータ区画の上部区域はインターフェースでロードされたトンネル定義の数である。メータ区画の照合IPトンネル・テーブルはディスプレイ区画でIPトンネルの照会明細と照合するインターフェースでロードされたトンネル定義の集合である。リスト区画のIPトンネル・テーブル構造はファイアウォールからロードされたトンネル定義の集合である。一時IPトンネル構造は、このページで管理者のアクションの結果として情報がIPトンネル定義ページに伝送される時に使用される選択IPトンネル定義を保持するため使用されるものである。

40

【0066】IPトンネル/フィルタ照会ページのデータ構造は、このページで情報のトラックを表示したり保存するために使用されたデータ構造を含む。ディスプレイ区画のIPトンネル・テーブル構造は、ファイアウォールからロードしたトンネル定義の集合であり、この情報はこのページでトンネルを画像表示するため使用している。ディスプレイ・アクション区画の照合フィルタ数は、ディスプレイ区画で選択されたIPトンネルIDと照合するインターフェースでロードしたIPフィルタ・ルールの数である。メータ区画の上部区域はインターフェースでロードされたフィルタ・ルールの数である。メ

50

ータ区画の照合フィルタ・ルール・テーブルはディスプレイ区画でIPトンネルのIDと照合するインターフェースでロードされたフィルタ・ルールの集合である。リスト区画のフィルタ・ルール・テーブル構造はファイアウォールからロードされたIPフィルタ・ルールの集合である。一時フィルタ・ルール構造は、このページで管理者のアクションの結果として情報がIPフィルタ定義ページに伝送される時に使用される選択フィルタ・ルールを保持するため使用されるものである。

【0067】データの他の組合せを有する他のデータ構造が別の実施例で使用できることは、当業者が容易に理解できることである。

【0068】図8には、IPトンネル定義ページの表示区画におけるユーザ入力により本システムが行うプロセスを示す。このプロセスはステップ1000で開始し、システムがユーザ入力を待ち受ける。ステップ1005では、区画ボタンが押されたかどうか判定する。YESならステップ1010で、組み合わせたエントリ・フィールドからの値がフェッチされる。ステップ1015は、組み合わせたエントリ・フィールドに値があるか判定する。NOならば、システムはステップ1000に戻る。YESなら、ピン・ボタンのプログラムはステップ1020でその値についておこなわれる。そしてプロセスはステップ1025に進み、ピン・ボタンのプログラムの出力は命令が実行される間、メータ区画に送られる。管理者はこのようにしてピン・ボタンによる操作が成功したか失敗か、見ることができる。このプロセスはステップ1000に戻り、ユーザの別のアクションを待機する。

【0069】ステップ1005の試験がNOなら、ステップ1030でトレースルート・ボタンが押されたか判定する。YESならステップ1035で、組み合わせたエントリ・フィールドからの値がフェッチされる。ステップ1040は、組み合わせたエントリ・フィールドに値があるか判定する。NOならば、システムはステップ1000に戻る。YESなら、トレースルート・ボタンのプログラムはステップ1045でその値についておこなわれる。そしてプロセスはステップ1025に進み、トレースルート・ボタンのプログラムの出力は命令が実行される間、メータ区画に送られる。このプロセスはステップ1000に戻る。

【0070】ステップ1030の試験がNOなら、ステップ1055で指ボタンが押されたか判定する。YESならステップ1060で、組み合わせたエントリ・フィールドからの値がフェッチされる。ステップ1065は、組み合わせたエントリ・フィールドに値があるか判定する。NOならば、システムはステップ1000に戻る。YESなら、指ボタンのプログラムはステップ1070でその値についておこなわれる。そしてプロセスはステップ1025に進み、指ボタンのプログラムの出力

は命令が実行される間、メータ区画に送られる。このプロセスはステップ1000に戻る。

【0071】ステップ1075で指ボタンが押されてないなら、ディスプレイ区画のエントリが修正されたかどうか判定する。YESなら、修正ビットをステップ1080でセットし、プロセスはステップ1000に戻る。NOならステップ1085でアクション理解不能とされ、このシステムは何も行わない。プロセスはステップ1000に戻り、ユーザ入力を待つ。

【0072】IPトンネル定義ページの表示アクション区画のユーザ入力に応じて行われるプロセスが図9に示されている。ステップ1100でプロセスが始まり、ユーザのアクションを待つ。ステップ1105では、クリア・ボタンが押されたか判定する。YESなら、ステップ1110で、ディスプレイ区画修正ビットがセットされているか判定する。YESなら、ステップ1115で、管理者はそのエントリを記憶させるか判断するように問われる。NOであれば、ステップ1120において、IPトンネル定義がディスプレイ区画から除去され、各フィールドは空白のままにされる。プロセスはステップ1100に戻りユーザの別の入力を待つ。しかし、管理者がエントリを記憶させると指示すると、プロセスはステップ1177に進み、そこで値をディスプレイ区画で検証する。

【0073】クリア・ボタンが押されてないなら、ステップ1125で、修正した選択エントリ・ボタンが押されているかどうか判定する。YESなら、ステップ1130で、ディスプレイ区画の値を検証する。ステップ1135では、検証で間違いがあったかどうか判定するためのテストを実行する。YESなら、ステップ1140で、その間違いをメータ区画に通知し、システムは1100に戻り、ユーザの別なアクションを待つ。間違いがない、つまりNOならば、ステップ1145で、検証の成功がメータ区画に表示される。プロセスはステップ1150に進み、エントリがリスト区画で選択されたかどうか判定する。YESならば、その選択されたエントリがディスプレイ区画からの値とリスト区画内で交換され、プロセスはステップ1100に戻る。NOならば、ステップ1160で同じIPトンネルIDを有するリスト・エントリがあるかどうか判定する。YESならば、ステップ1165で、同じIDを有するIPトンネル・エントリはディスプレイ区画の値でリスト区画内において交換される。プロセスはユーザのアクションの待機を再開する。同じIPトンネルIDを有するエントリが無ければ、ステップ1170でディスプレイ区画の値がリスト区画の新たな列として加えられる。プロセスはステップ1100に戻る。

【0074】ステップ1175で、選択したエントリを加える、というボタンが押されたかどうか判定する。YESならば、ステップ1177で、ディスプレイ区画の

値を検証する。ステップ1180では、検証で間違いがあったかどうか判定するためのテストを実行する。なんらかの間違いがあるなら、ステップ1185で、その間違いをメータ区画に通知し、システムは1100に戻る。間違いがない、つまりNOならば、ステップ1190で、検証の成功がメータ区画に表示され、プロセスはステップ1160に進む。

【0075】ステップ1105、1125、1175での判定テストが全て不成功なら、ステップ1195でアクション認識不能とされ、このシステムは何も行わない。プロセスはステップ1100に戻り、ユーザ入力を待つ。

【0076】図10には、IPトンネル定義ページのリスト区画におけるユーザ入力に応じたプロセスが示されている。ステップ1200でプロセスが始まり、ユーザのアクションを待つ。ステップ1205では、リスト区画エントリが選択されたか判定する。YESなら、ステップ1210で、ディスプレイ区画修正ビットがセットされているか判定する。YESなら、ステップ1215で、管理者はそのエントリを記憶させるか判断するように問われる。NOであれば、ステップ1213でリスト区画からの選択エントリとディスプレイ区画の内容が交換させられ、システムはステップ1200に戻る。管理者がディスプレイ区画の値を記憶させると指示すると、プロセスはステップ1220に進み、そこでディスプレイ区画の値を検証する。ステップ1225では、検証で間違いがあったかどうか判定するためのテストを実行する。なんらかの間違いがあるなら、ステップ1230で、その間違いをメータ区画に通知し、システムは1200に戻る。間違いがない、つまりNOならば、ステップ1235で、検証の成功がメータ区画に表示され、プロセスはステップ1240に進む。ステップ1240では、ディスプレイ・ページからのと同じトンネルIDを有するリスト・エントリがあるか判定する。あるなら、ステップ1245でIPトンネル・エントリはリスト区画でディスプレイ区画値を有する同じIDと交換される。この場合、管理者は既に存在するトンネル定義を修正している。ステップ1240の判定がNOなら、ステップ1250でディスプレイ区画の値がリスト区画内の新たな列として加えられる。

【0077】ステップ1205でNOなら、ステップ1255でアクション認識不能とされ、処理はステップ1200に続く。

【0078】図11、図12には、IPトンネル定義ページのリスト・アクション区画におけるユーザ入力によって行われるプロセスを示す。ステップ1300でプロセスが始まり、ユーザの入力を待つ。ステップ1303では、エントリ削除ボタンが押されたか判定する。YESなら、ステップ1305で、エントリがリスト区画で選択されたか判定する。NOなら、システムはステップ

1300に戻りユーザの別の入力を待つ。エントリがステップ1310で選択されたなら、リスト区画からその選択エントリを除去する。ステップ1313で、エントリの削除がIPトンネル定義ページのメータ区画に通知される。プロセスはステップ1300に戻る。

【0079】ステップ1315では、エントリ活性化ボタンが押されたか判定する。YESなら、ステップ1320で、エントリがリスト区画で選択されたか判定する。NOなら、システムはステップ1300に戻る。エントリがステップ1325で選択されたなら、選択したIPトンネル・エントリの活性属性を活性にセットする。プロセスはステップ1300に戻りユーザのアクションを待つ。活性トンネルとは、IPトンネルを通じてパケットと照合する経路をつくるためにフィルタ・ルールが定義されている時、ファイアウォールが複数のIPパケットを送ることのできるものである。IPトンネルは定義可能であるが、複数のIPパケットを受け入れるために活性にはできない。

【0080】ステップ1330では、エントリ不活性化ボタンが押されたか判定する。YESなら、ステップ1333で、エントリがリスト区画で選択されたか判定する。NOなら、システムはステップ1300に戻りユーザのアクションを待つ。エントリがステップ1335で選択されたなら、選択したIPトンネル・エントリの活性属性を不活性化にセットする。プロセスはステップ1300に戻りユーザのアクションを待つ。

【0081】ステップ1339では、からロードというボタンが押されたか判定する。YESなら、ステップ1340で、管理者はどのファイアウォールからIPトンネル定義をロードするか問われる。ステップ1345で、特定のファイアウォールからのIPトンネル定義がロードされる。ステップ1350では、ロード処理で誤りがあるかどうか判定する。誤りがあるなら、ステップ1355で、誤りをメータ区画に通知する。誤りがないなら、ステップ1360で、ロード処理の成功をメータ区画に通知する。ステップ1365では、リスト区画エントリはロードしたIPトンネル・リストと交換される。ステップ1369では、ディスプレイ区画エントリはクリアされる。ステップ1370では、ディスプレイ区画修正ビットがセット・オフされる。プロセスはステップ1300に戻りユーザの入力を待つ。

【0082】ステップ1373では、ファイアウォールへ保存というボタンが押されたか判定する。YESなら、ステップ1375で、管理者はどのファイアウォールへIPトンネル定義を保存するか問われる。ステップ1377で、特定されたファイアウォールへIPトンネル定義を保存する。ステップ1379では、保存の結果をメータ区画に通知する。プロセスはステップ1300に戻る。

【0083】図13では、ステップ1380において、

ファイアウォール活動停止というボタンが押されたか判定する。このボタンが押されたなら、ステップ1385でファイアウォールの全てのIPトンネル定義は停止あるいは不活性とされる。ステップ1387で、停止の結果をメータ区画に通知する。

【0084】ステップ1390で、ファイアウォール間で検証というボタンが押されたか判定する。このボタンが押されたなら、ステップ1393でファイアウォール間、つまりソースファイアウォールと目標ファイアウォール間のトンネル定義をIPトンネル・リストで検証される。検証プロセスはファイアウォールにより提供されたものと同じである。ステップ1397で、システムはこのアクションは理解不能であると判定し、何も行わない。この時点で、プロセスはステップ1300に戻り、ユーザの別な入力待つ。

【0085】IPトンネル画像ページの表示アクション区画のユーザ入力に応じて行われるシステム・アクションを図14に示している。ステップ1400でプロセスが始まり、ユーザの入力を待つ。ステップ1405では、全てを見せるというボタンが押されたか判定する。YESなら、ステップ1410で、ディスプレイ区画の画像が書き直され、全てのIPトンネルを見せる。ステップ1415では、活動中のものを見せるというボタンが押されたか判定する。YESなら、ステップ1420で、ディスプレイ区画で画像が書き直され、活動中のIPトンネル接続を明るく点灯する。プロセスはステップ1400に戻る。ステップ1425で、非活動中のものを見せるというボタンが押されたか判定する。YESなら、ステップ1423で、ディスプレイ区画で画像が書き直され、非活動中のIPトンネル接続を明るく点灯する。ステップ1435で、このシステムはユーザ入力30が不明のアクションとして分類し、ステップ1400に戻りユーザの別な入力待つ。

【0086】図15、図16はIPトンネル画像ページにおけるリスト・アクション区画の入力からのシステム・アクションを示す。ステップ1500でプロセスが始まり、ユーザの入力を待つ。ステップ1503では、エントリ編集ボタンが押されたか判定する。YESなら、ステップ1505で、エントリがリスト区画で選択されたか判定する。NOなら、システムはステップ1500に戻りユーザの別な入力待つ。エントリがステップ1507で選択されたなら、その選択エントリの内容を一時IPトンネル定義構造に記憶させる。ステップ1509で、IPトンネル定義ページが表示される。ステップ1510で、一時IPトンネル定義の内容がディスプレイ区画に表示され、プロセスは図11、図12、図13、図14、図15、図16に示したIPトンネル定義ページのアクションに進む。

【0087】ステップ1515では、エントリ削除ボタンが押されたか判定する。YESなら、ステップ151

7で、エントリがリスト区画で選択されたか判定する。NOなら、システムはステップ1500に戻りユーザの別の入力待つ。エントリがステップ1517で選択されたなら、ステップ1519でリスト区画からその選択エントリを除去し、ステップ1520ではリスト区画修正ビットをセット・オンする。ステップ1523では、IPトンネル画像が書き直され、リスト区画の新しい内容を反映させる。プロセスはステップ1500に戻る。

【0088】ステップ1525では、エントリ活性化ボタンが押されたか判定する。YESなら、ステップ1529で、エントリがリスト区画で選択されたか判定する。エントリが選択されたなら、選択したエントリのIPトンネル定義をステップ1530で活性化し、プロセスはステップ1520にもどる。

【0089】ステップ1535で、エントリ不活性化ボタンが押されたか判定する。YESなら、ステップ1539で、エントリがリスト区画で選択されたか判定する。エントリが選択されたなら、選択したエントリのIPトンネル定義をステップ1540で不活性化し、プロセスはステップ1520にもどり、リスト区画修正ボタンをセットし、ステップ1523でIPトンネル画像を描き直す。

【0090】ステップ1545では、ファイアウォールからロードというボタンが押されたか判定する。YESなら、ステップ1550で、リスト区画修正ビットがオンか判定する。NOであれば、ステップ1553で、管理者はどのファイアウォールからロードするか問われる。ステップ1555で、特定したファイアウォールからのIPトンネル定義がロードされる。ステップ1560では、ロード処理で誤りがあるかどうか判定する。誤りがあるなら、ステップ1563で、誤りをチャッカ・テーブル区画に通知し、プロセスはステップ1500に戻る。誤りがないなら、ステップ1565で、ロード処理の成功をチャッカ・テーブル区画に通知する。ステップ1570では、リスト区画のIPトンネルリストをロードしたIPトンネル・リストと交換する。ステップ1573では、リスト区画修正ビットがセット・オフされる。プロセスはステップ1523に戻り、IPトンネル画像がディスプレイ区画で書き直される。

【0091】ステップ1575では、管理者は現在のリスト区画内容を保存するか問われる。管理者がそのリスト区画内容を保存すると指示したら、ステップ1580で、その内容が目標ファイアウォールのIPトンネル・テーブルとして保存される。ステップ1583では、その結果をチャッカ・テーブル区画に通知する。この時点で、プロセスはステップ1553に戻り、管理者にどのファイアウォールからロードするか問う。

【0092】図17のステップ1585では、ファイアウォールへ保存というボタンが押されたか判定する。YESなら、ステップ1590で、管理者はどのファイア

ウォールへ保存するか問われる。ステップ1593で、特定したファイアウォールヘリスト区画のIPトンネル定義を保存する。ステップ1595では、保存の結果をチェック・テーブル区画に通知する。プロセスはステップ1500に戻りユーザの入力を待つ。ステップ1597で、このアクションは不明アクションとして分類され、プロセスはステップ1500に戻りユーザの入力を待つ。

【0093】図18はIPトンネル照会ページの表示アクション区画におけるユーザ入力により行われるシステム・アクションを示すフローチャートである。ステップ1600でプロセスが始まり、ユーザの入力を待つ。ステップ1605では、クリア・ボタンが押されたか判定する。YESなら、ステップ1610で、IPトンネル値がディスプレイ区画から除去される、つまりエントリ・フィールドは空白である。ステップ1615では、メータ区画のリンクしたリストがクリアされ、メータ区画が表示される。ステップ1620では、チェック・テーブル区画がクリアされる。ステップ1625では、ディスプレイ・アクション区画で照合した数としてゼロが表示される。プロセスはステップ1600に戻り、ユーザのアクションを待つ。

【0094】ステップ1630では、照会実行ボタンが押されたか判定する。押されたなら、ステップ1635で、メータ区画リンク・リストがクリアされ、IPトンネル・テーブルを介してカウンタを増加するため使用する変数*i*を1にセットする。ステップ1640では、*i*がIPトンネル・テーブルのIPトンネルの数より大きいか判定する。大きくないなら、ステップ1645でIPトンネル・テーブルがIPトンネル・エントリの照会明細と照合しているか判定する。これはリスト区画の指標列に対してディスプレイ区画の入力を照合させることにより行われる。ステップ1650では、*i*による指標のIPトンネル・テーブルはメータ区画リンク・リストに加えられる。ステップ1655では、*i*が1増加し、プロセスはステップ1640に戻る。*i*がIPトンネル・テーブルのIPトンネルの数を越えるなら、ステップ1660ではメータ区画リンク・リストがエントリを有するか判定する。YESなら、ステップ1665において、照合するエントリにメータ区画内で陰影を着ける。結果をチェック・テーブル区画ステップ1670に表示し、ステップ1675では、照合した数をディスプレイ・アクション区画に表示する。プロセスはステップ1600に戻りユーザのアクションを待つ。ステップ1680では、このアクションは認識されず、プロセスはステップ1600に戻る。

【0095】図19では、IPトンネル照会ページのリスト区画に対するユーザ入力に応じて行うシステム・アクションを示す。ステップ1700でユーザ入力を待つ。ステップ1705では、エントリが選択されたか判

定する。選択されたなら、ステップ1710で、エントリをディスプレイ区画で交換する。ディスプレイ・アクション照合数はステップ1715で「ゼロ」に変わる。次に、ステップ1720で、メータ区画リンク・リストがクリアされ、メータ区画での陰影もクリアされる。ステップ1700に戻り、ユーザ・アクションを待つ。

【0096】ステップ1725では、リストがリスト区画でスクロールされたか判定する。YESなら、ステップ1730でメータ区画の位置キューの垂直バーがリスト区画で示されているものと照合するように変えられる。プロセスはステップ1700に戻る。ステップ1735では、このアクションは不明とされ、何も行わない。そして、ステップ1700に戻り、ユーザのアクションを待つ。

【0097】IPトンネル照会ページのリスト・アクション区画におけるユーザ入力に応じたシステムのアクションが図20に示されている。ステップ1800で、ユーザ入力を待つ。ステップ1805では、編集ボタンが押されたか判定する。YESなら、ステップ1810で、リスト区画にエントリがあるか、またそれは選択されたか判定される。NOならば、システムはステップ1800に戻る。YESなら、ステップ1815で、選択エントリの内容を一時IPトンネル定義構造に記憶させる。ステップ1820で、IPトンネル定義ページが表示され、ステップ1825で、一時IPトンネル定義構造の内容がディスプレイ区画に置かれる。次に、システムはステップ1830の図10、11、12、13、14、15、16に関連して説明したIPトンネル定義ページ・アクションに進む。

【0098】ステップ1835で、IPトンネルをロードするというボタンが押されたか判定する。YESなら、ステップ1840で、ファイアウォールから記憶させたIPトンネル定義をロードする。ステップ1845で、新たなIPトンネル・テーブルをリスト区画に表示する。プロセスはステップ1800に戻る。

【0099】ステップ1850で、このアクションは認識せずと判定し、何も行わない。プロセスはステップ1800に戻り、ユーザ入力を待つ。

【0100】図21は、IPトンネル/フィルタ照会ページの表示アクション区画におけるユーザ入力に応じたシステム・アクションを示す。ステップ1900で、ユーザ入力を待つ。ステップ1905で、クリア・ボタンが押されたか判定する。YESなら、ステップ1910で、明るい点灯を画像およびディスプレイ区画から除去する。ステップ1915で、メータ区画リンク・リストはクリアされ、メータ区画が再度表示される。ステップ1920で、チェック・テーブル区画がクリアされる。ステップ1925で、ディスプレイ・アクション区画で照合したフィルタの数としてゼロが表示され、選択したIPトンネルの数が表示され、プロセスはステップ1900

に戻る。

【0101】ステップ1930で、照会実行のボタンが押されたか判定する。押されたのなら、ステップ1935で、メータ区画リンク・リストがクリアされ、変数*i*を1にセットする。ステップ1940では、*i*がリスト区画のIPフィルタ・ルールの数より大きいと判定する。大きくないなら、ステップ1945でIPフィルタ・テーブルが、ディスプレイ区画で選択IDトンネルと照合するトンネルIDを有するか判定する。YESなら、ステップ1950で、IPフィルタ・テーブルの*i*による指標のトンネル定義がメータ区画リンク・リストに加えられる。ステップ1955では、変数*i*が増加させられる。

【0102】ステップ1960で、メータ区画リンク・リストがエントリを有するか判定する。YESなら、ステップ1965において、照会定義と照合するメータ・リスト・エントリにメータ区画内で陰影を着ける。1970で、結果をチャック・テーブル区画に表示し、ステップ1975では、フィルタと照合した数をディスプレイ・アクション区画に表示する。プロセスはステップ1900に戻る。

【0103】ステップ1980では、このアクションは認識されず、プロセスはステップ1900に戻り、ユーザの別なアクションを待つ。

【0104】図22は、IPトンネル/フィルタ照会ページのリスト区画へのユーザ入力によるシステム・アクションを示す。ステップ2000で、ユーザ入力待つ。ステップ2005で、エントリが選択されたか判定する。YESなら、ステップ2010でディスプレイ・アクション照合数が「ゼロ」に変わる。選択したIPトンネルをディスプレイ・アクション区画から除去する。ステップ2015では、メータ区画リンク・リストがクリアされ、メータ区画を再度表示する。ステップ2020では、明るい点灯をディスプレイ区画の選択エントリから除去する。

【0105】ステップ2025では、リストがスクロールされたか判定する。YESなら、ステップ2030で、メータ区画の垂直バーの位置キューを、リスト区画に示されているものと照合するように変える。ステップ2035では、このアクションは不明とする。プロセスはステップ2000に戻り、ユーザ入力待つ。

【0106】図23は、IPトンネル/フィルタ照会ページのリスト・アクション区画に対するユーザ入力に応じたシステム・アクションを示す。ステップ2100で、ユーザ入力待つ。ステップ2105で、エントリ編集ボタンが押されたか判定する。YESなら、ステップ2110でリスト区画のエントリが選択されたか判定する。NOなら、システムはステップ2100に戻り、ユーザ・アクションを待つ。ステップ2115では、選択したエントリの内容を一時IPフィルタ・ルール構造

に記憶する。ステップ2120で、IPフィルタ定義ページが表示される。ステップ2125では、一時IPフィルタ・ルール構造の内容をディスプレイ区画に表示し、ステップ2130では前述の引例に説明があるIPフィルタ定義ページ・アクションに進む。

【0107】ステップ2135では、フィルタ・リストをロードするというボタンが押されているか判定する。YESなら、ステップ2140でファイアウォールからのこれらのIP/フィルタ定義を記憶させる。ステップ2145では、新たなIPフィルタ・テーブルをリスト区画に示す。ステップ2150では、このアクションは不明とし、アクションはとらない。プロセスはステップ2100に戻る。

【0108】上記の説明はIPトンネリングおよびフィルタ処理、つまり種々のインターネット本体により公表されたトンネル・ルールおよびフィルタ・ルールに関するものであり、本発明は安全なネットワークと安全でないネットワーク間に課することの可能なトンネル・ルールとフィルタ・ルールの集合への応用である。例えば、マイクロソフト社によって初め提案されたポイント対ポイント・トンネリング・プロトコルは、本発明の使用により最小限の改修で管理可能となる。

【0109】本発明の特定の実施例について示し、説明を行ったが、本発明が修正により他の環境においても実施可能であることは当業者に容易に理解されるであろう。例えば、上記説明の本発明は選択的に改変したりソフトウェアにより作動させた、汎用コンピュータにおいて容易に実行可能であるが、本発明はハードウェア、ファームウェア、あるいはソフトウェア、ファームウェアまたは上記の本発明を実現するため特別設計した特殊な装置を含むハードウェアのいかなる組合せでも実行可能であることは、当業者は容易に理解できる。従って、形態および細部の変更は前述の請求の範囲の精神および範囲を逸脱しない限り、行えるものである。

【0110】まとめとして、本発明の構成に関して以下の事項を開示する。

【0111】(1) 安全なコンピュータ・ネットワークと安全でないコンピュータ・ネットワーク間のファイアウォール・コンピュータにおけるトンネリングを管理する方法において、複数のネットワークのアドレス間のトンネルのグラフィック図をネットワーク・アドレスを示すアイコンを接続するラインとして表示するステップと、第一ラインのユーザの選択に応じて、その第一ラインによって示された選択したトンネル定義を表示するステップと、ユーザ入力に応じて、上記選択したトンネル定義へのアクションを行うステップとを有することとを特徴とするファイアウォール・コンピュータのトンネリングを管理する方法。

(2) 上記トンネルのグラフィック図は、ユーザ入力により、全ての定義したトンネルを示し、活動中のトンネ

ルを示し、あるいは非活動中のトンネルを示すように選択的に変えることが可能であることを特徴とする、上記(1)に記載の方法。

(3) 上記ラインは、各々のトンネルの特性を示す異なった方法で描かれていることを特徴とする、上記(1)に記載の方法。

(4) 上記特性はトンネルに可能な安全状態であることを特徴とする、上記(3)に記載の方法。

(5) 上記グラフィック図は各トンネルが発生してくる方向を示す印を有することを特徴とする、上記(1)に記載の方法。

(6) 安全なコンピュータ・ネットワークと安全でないコンピュータ・ネットワーク間のファイアウォール・コンピュータのトンネリングを管理する方法において、トンネル定義を入れることのできる第一区画を有するユーザ・インターフェースを示すステップと、ユーザ入力に応じて、入力されたトンネル定義と既存のトンネル定義が照合するか判定するために、入力されたトンネル定義についての照会を実行するステップと、上記照会の結果を分散バーでユーザ・インターフェースの別な区画に表示し、トンネル定義の照合の位置は分散バーを通るラインにより示されるステップと、ユーザ入力に応じて、選択トンネル定義についてのアクションを行うステップとを有することを特徴とするファイアウォール・コンピュータのトンネリングを管理する方法。

(7) 第三区画でトンネル定義のリストを表示し、そこでは照合するトンネル定義が照合しないトンネル定義とは異なった方法で表示するステップと、上記分散バーに隣接し、上記分散バーによって示されたトンネル定義の完全なリストに関して第三区画に表示したトンネル定義のリストの位置を示す小さなバーを表示するステップとを、さらに有することを特徴とする上記(6)に記載の方法。

(8) 上記分散バーに隣接し、照合するトンネル定義の集中を示す小さなバーを表示するステップを、さらに有することを特徴とする上記(6)に記載の方法。

(9) 安全なコンピュータ・ネットワークと安全でないコンピュータ・ネットワーク間のファイアウォール・コンピュータのトンネリングを管理する方法において、複数のネットワークのアドレス間のトンネルのグラフィック図をネットワーク・アドレスを示すアイコンを接続するラインとして表示するステップと、第一ラインのユーザの選択に応じて、その第一ラインによって示された選択したトンネルに適用できるフィルタ・ルールのリストを表示するステップと、ユーザ入力に応じて、上記選択したフィルタ・ルールへのアクションを行うステップとを有することを特徴とするファイアウォール・コンピュータのトンネリングを管理する方法。

(10) ユーザ入力に応じて、選択したトンネルに既存のフィルタ・ルールが応用可能か判定するために、選択

したトンネルについての照会を実行するステップと、上記照会の結果を分散バーでユーザ・インターフェースの別な区画に表示し、フィルタ・ルールの照合の位置は分散バーを通るラインにより示されるステップとを更に有することを特徴とする、上記(9)に記載の方法。

(11) 照合するフィルタ・ルールを、フィルタ・ルールのリストの照合しないフィルタ・ルールとは異なった方法で表示するステップと、上記分散バーに隣接し、上記分散バーによって示されたフィルタ・ルールの完全なリストに関して第三区画に表示したフィルタ・ルールのリストの位置を示す小さなバーを表示するステップとを、さらに有することを特徴とする上記(10)に記載の方法。

(12) 安全なコンピュータ・ネットワークと安全でないコンピュータ・ネットワーク間のファイアウォール・コンピュータのトンネリングを管理するためのプロセッサとメモリを有するシステムにおいて、複数のネットワークのアドレス間のトンネルのグラフィック図をネットワーク・アドレスを示すアイコンを接続するラインとして表示する手段と、第一ラインのユーザの選択に応じて、その第一ラインによって示された選択したトンネル定義を表示する手段と、ユーザ入力に応じて、上記選択したトンネル定義へのアクションを行う手段とを有することを特徴とするファイアウォール・コンピュータのトンネリングを管理するシステム。

(13) 上記トンネルのグラフィック図は、ユーザ入力により、全ての定義したトンネルを示し、活動中のトンネルを示し、あるいは非活動中のトンネルを示すように選択的に変えることが可能であることを特徴とする、上記(12)に記載のシステム。

(14) 上記ラインは、各々のトンネルの特性を示す異なった方法で描かれていることを特徴とする、上記(12)に記載のシステム。

(15) 上記特性はトンネルに可能な安全状態であることを特徴とする、上記(14)に記載のシステム。

(16) 上記グラフィック図は各トンネルが発生してくる方向を示す印を有することを特徴とする、上記(12)に記載のシステム。

(17) 安全なコンピュータ・ネットワークと安全でないコンピュータ・ネットワーク間のファイアウォール・コンピュータのトンネリングを管理するためのプロセッサとメモリを有するシステムにおいて、トンネル定義を入力することのできる第一区画を有するユーザ・インターフェースを示す手段と、ユーザ入力に応じて、入力されたトンネル定義と既存のトンネル定義が照合するか判定するために、入力されたトンネル定義についての照会を実行する手段と、上記照会の結果を分散バーでユーザ・インターフェースの別な区画に表示し、トンネル定義の照合の位置は分散バーを通るラインにより示される手段と、ユーザ入力に応じて、選択トンネル定義について

のアクションを行う手段とを有することを特徴とするファイアウォール・コンピュータのトンネリングを管理するシステム。

(18) 第三区画でトンネル定義のリストを表示し、ここでは照合するトンネル定義が照合しないトンネル定義とは異なった方法で表示する手段と、上記分散バーに隣接し、上記分散バーによって示されたトンネル定義の完全なリストに関して第三区画に表示したトンネル定義のリストの位置を示す小さなバーを表示する手段とを、さらに有することを特徴とする上記(17)に記載のシステム。

(19) 上記分散バーに隣接し、照合するトンネル定義の集中を示す小さなバーを表示する手段とを、さらに有することを特徴とする上記(17)に記載のシステム。

(20) 安全なコンピュータ・ネットワークと安全でないコンピュータ・ネットワーク間のファイアウォール・コンピュータのトンネリングを管理するプロセッサとメモリを有するシステムにおいて、複数のネットワークのアドレス間のトンネルのグラフィック図をネットワーク・アドレスを示すアイコンを接続するラインとして表示する手段と、第一ラインのユーザの選択に応じて、その第一ラインによって示された選択したトンネルに応用できるフィルタ・ルールのリストを表示する手段と、ユーザ入力に応じて、上記選択したフィルタ・ルールへのアクションを行う手段とを有することを特徴とするファイアウォール・コンピュータのトンネリングを管理するシステム。

(21) ユーザ入力に応じて、選択したトンネルに既存のフィルタ・ルールが応用可能か判定するために、選択したトンネルについての照会を実行する手段と、上記照会の結果を分散バーでユーザ・インターフェースの別な区画に表示し、フィルタ・ルールの照合の位置は分散バーを通るラインにより示される手段とを更に有することを特徴とする、上記(20)に記載の方法。

(22) 照合するフィルタ・ルールを、フィルタ・ルールのリストの照合しないフィルタ・ルールとは異なった方法で表示する手段と、上記分散バーに隣接し、上記分散バーによって示されたフィルタ・ルールの完全なリストに関して第三区画に表示したフィルタ・ルールのリストの位置を示す小さなバーを表示する手段とを、さらに有することを特徴とする上記(21)に記載の方法。

【図面の簡単な説明】

【図1】本発明により構成されたコンピュータ・システムの構成図である。

【図2】本発明が使用される環境の一実施例を示す概略図である。

【図3】本発明が使用される環境の別の実施例を示す概略図である。

【図4】ウェブ・ベースのユーザ・インターフェースにおけるIPトンネル定義のページを示す表示例。

【図5】ウェブ・ベースのユーザ・インターフェースにおけるIPトンネルのグラフィック・ページを示す表示例。

【図6】ユーザ・インターフェースにおけるIPトンネル照会ページを示す表示例。

【図7】ユーザ・インターフェースにおけるIPトンネル/フィルタ照会ページを示す表示例。

【図8】IPトンネル定義ページの表示区画とアクションを示すフローチャート。

10 【図9】IPトンネル定義ページの表示アクション区画のアクションを示すフローチャート。

【図10】IPトンネル定義ページのリスト区画におけるユーザ入力に従うアクションを示すフローチャート。

【図11】IPトンネル定義ページのリスト・アクション区画におけるユーザ入力によって取るアクションを示すフローチャートの前半部分。

【図12】図11のフローチャートの後半部分。

【図13】図12に続くフローチャート。

20 【図14】IPトンネル画像ページの表示アクション区画のユーザ入力に応じるプロセスを示すフローチャート。

【図15】IPトンネル画像ページにおけるリスト・アクション区画の入力からのシステム・アクションを示すフローチャートの前半部分。

【図16】図15のフローチャートの後半部分。

【図17】図16に続くフローチャート。

【図18】IPトンネル照会ページの表示アクション区画におけるユーザ入力により取られるシステム・プロセスを示すフローチャート。

30 【図19】IPトンネル照会ページのリスト区画における入力により取られるアクションを示すフローチャート。

【図20】IPトンネル照会ページのリスト・アクション区画におけるユーザ・アクションに応じたシステムのアクションを示すフローチャート。

【図21】IPトンネル/フィルタ照会ページの表示アクション区画における入力に応じたシステム・アクションを示すフローチャート。

40 【図22】IPトンネル/フィルタ照会ページのリスト区画から取られるアクションを示すフローチャート。

【図23】IPトンネル/フィルタ照会ページのリスト・アクション区画におけるユーザ・アクションに応じたシステム・アクションを示すフローチャート。

【符号の説明】

11 システム・ユニット

12 キーボード

13 マウス

14 ディスプレイ

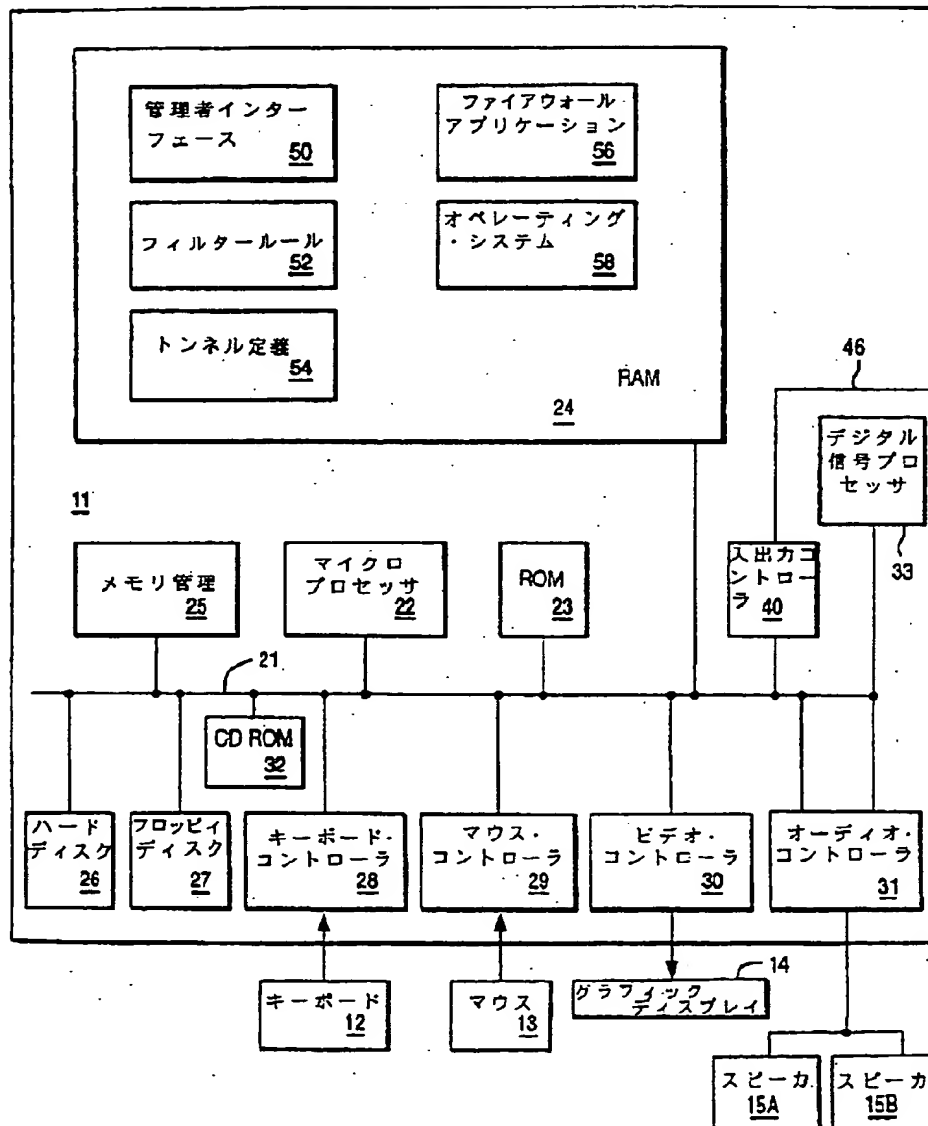
21 システム・バス

50 22 マイクロプロセッサ

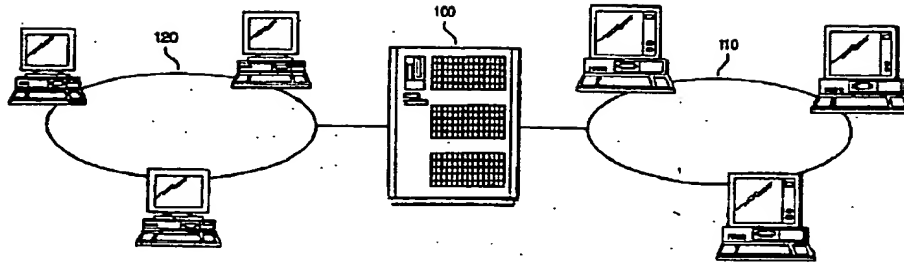
31
 23 読取り専用メモリ (ROM)
 24 ランダム・アクセス・メモリ (RAM)
 25 メモリ管理チップ
 26 ハード・ディスク・ドライブ
 27 フロッピー・ディスク・ドライブ
 28 キーボード・コントローラ
 29 マウス・コントローラ
 30 ビデオ・コントローラ
 31 オーディオ・コントローラ
 32 CD-ROM
 40 入力/出力コントローラ
 200 ナビゲーション区画

32
 * 210 ディスプレイ区画
 212 エントリ・フィールド
 214 押しボタン
 216 スクロール・バー
 220 ディスプレイ・アクション区画
 230 メータ区画
 240 リスト区画
 244 スクロール・バー
 246 スクロール・バー
 10 250 リスト・アクション区画
 252 押しボタン
 * 260 チッカ・テープ区画

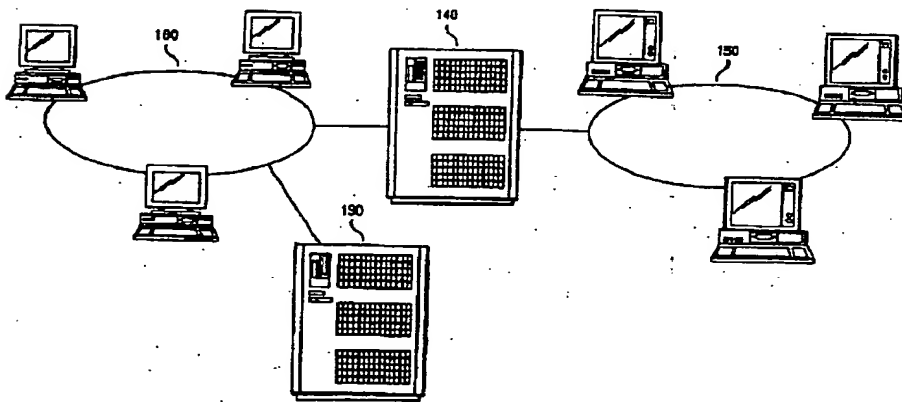
【図1】



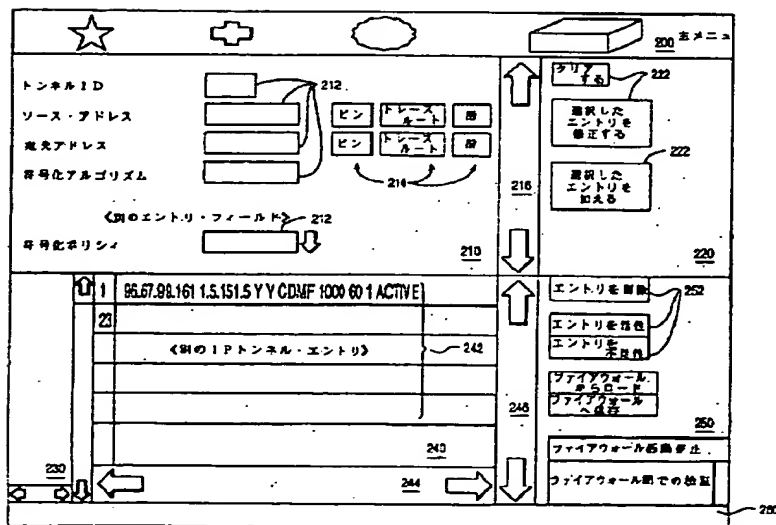
【図2】



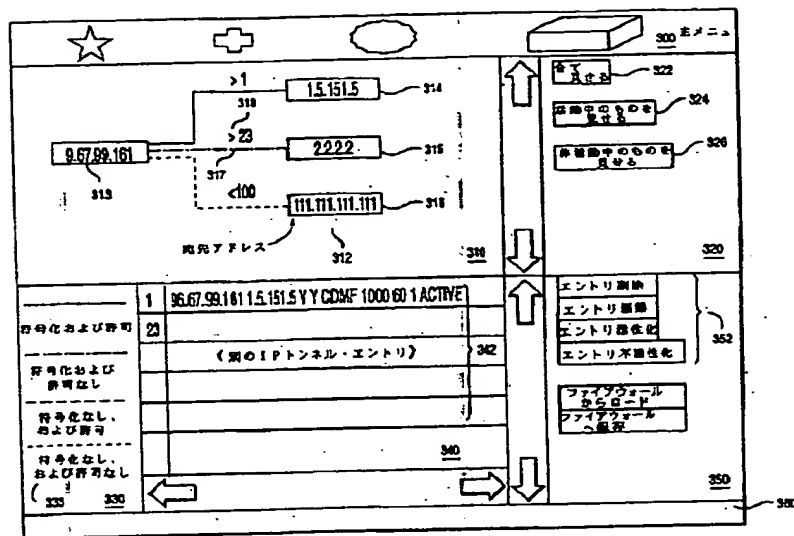
【図3】



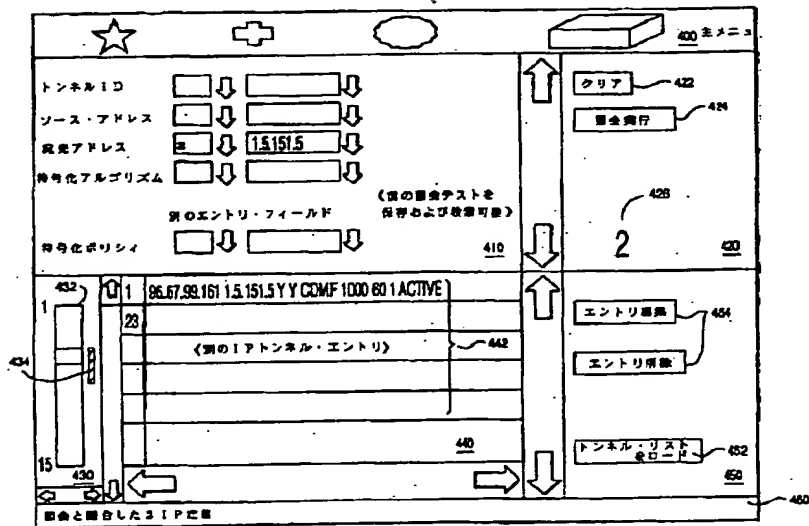
【図4】



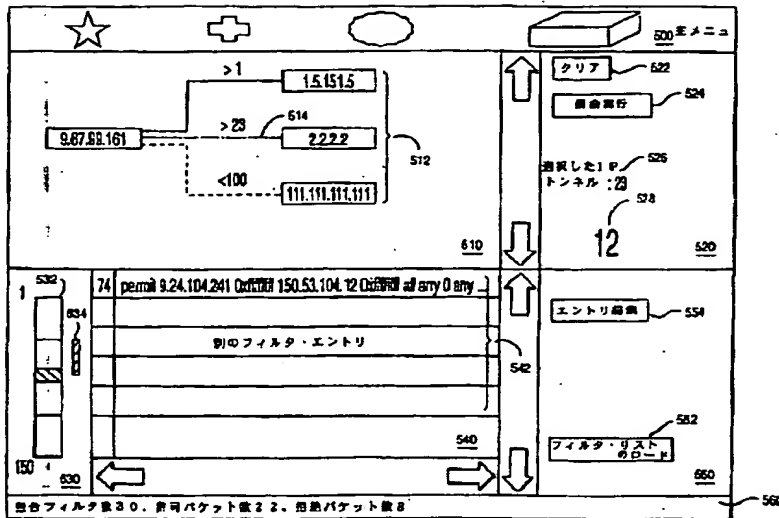
【図5】



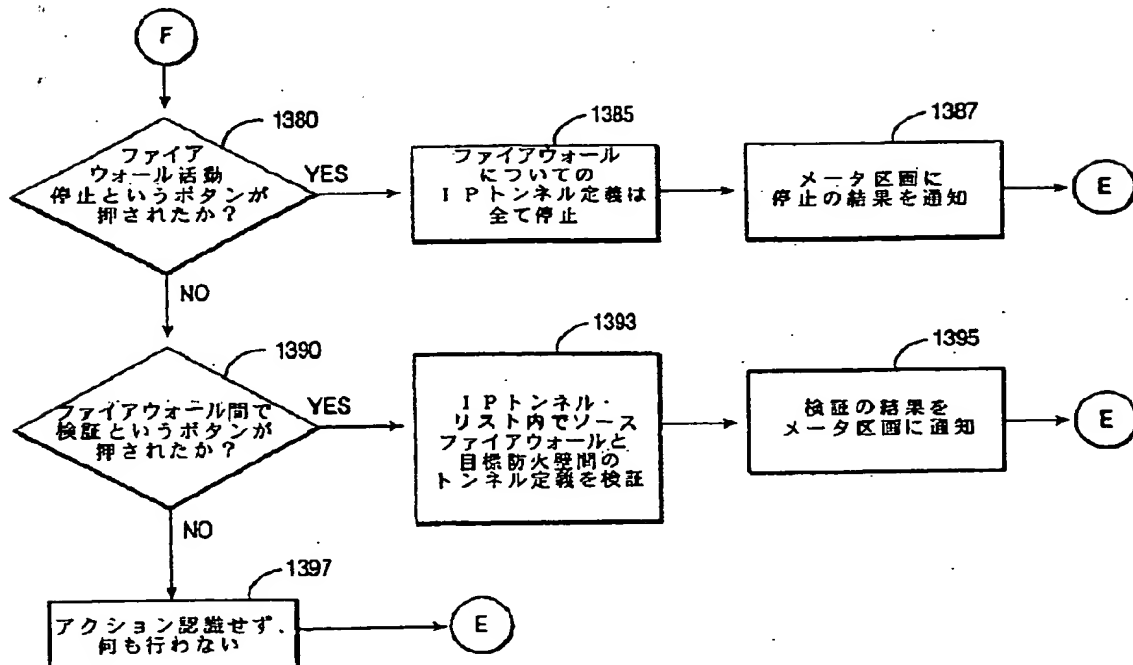
【図6】



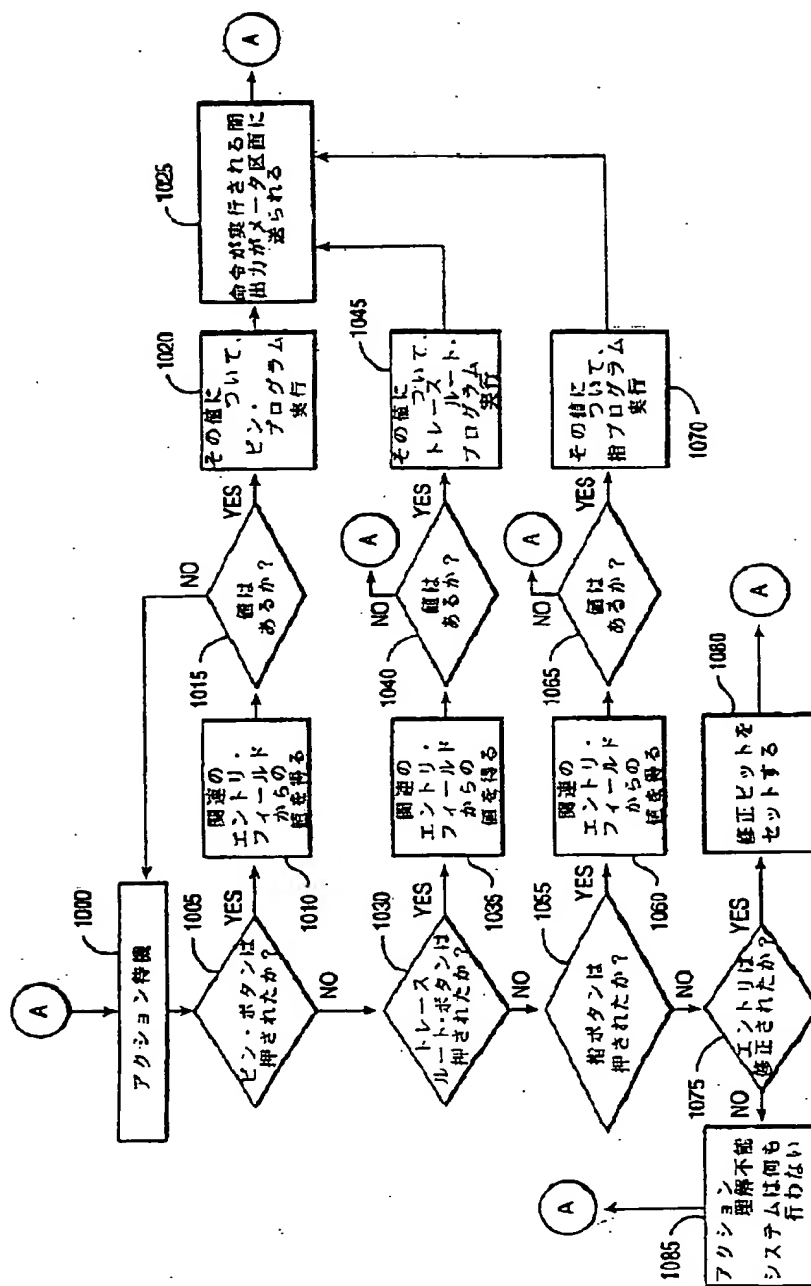
【図7】



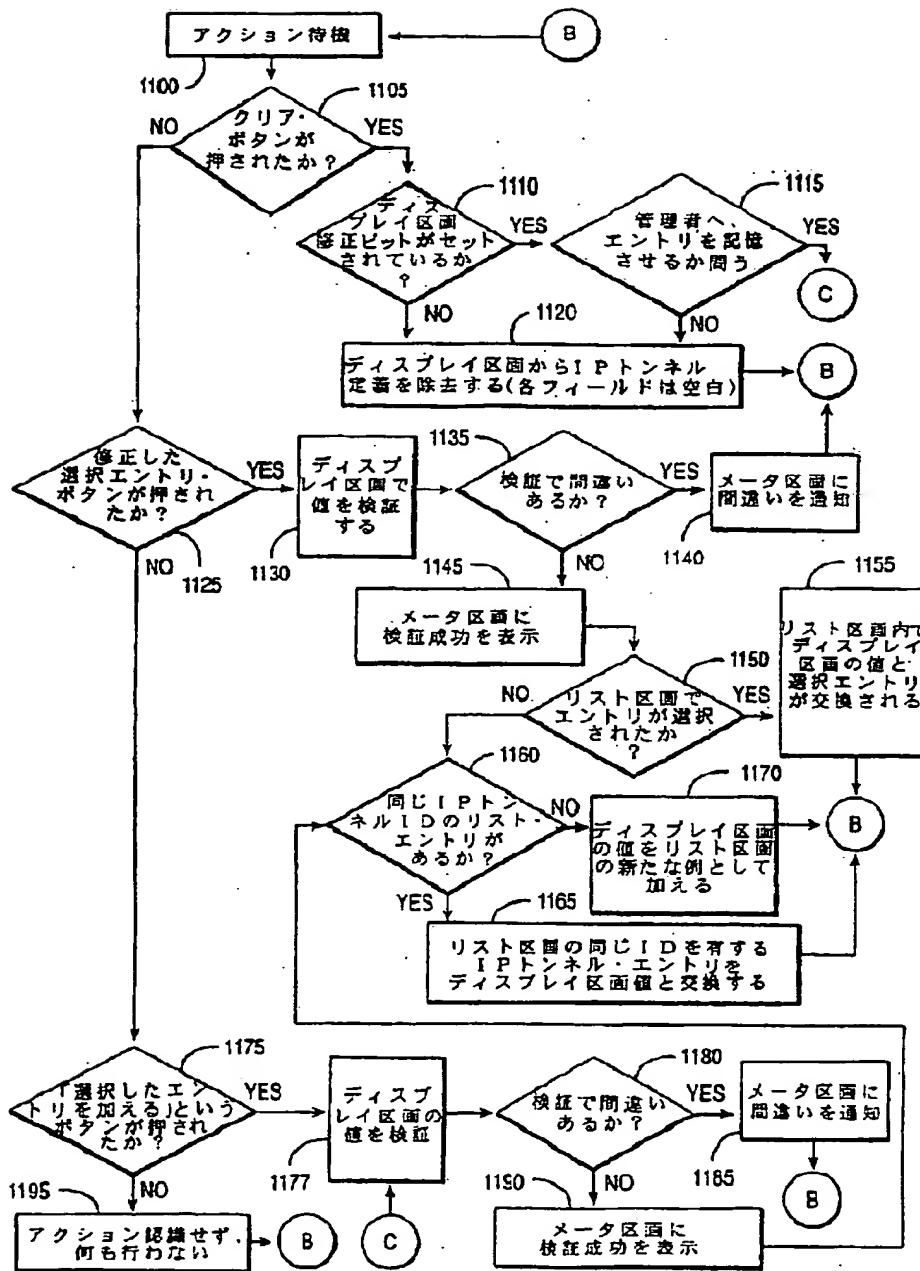
【図13】



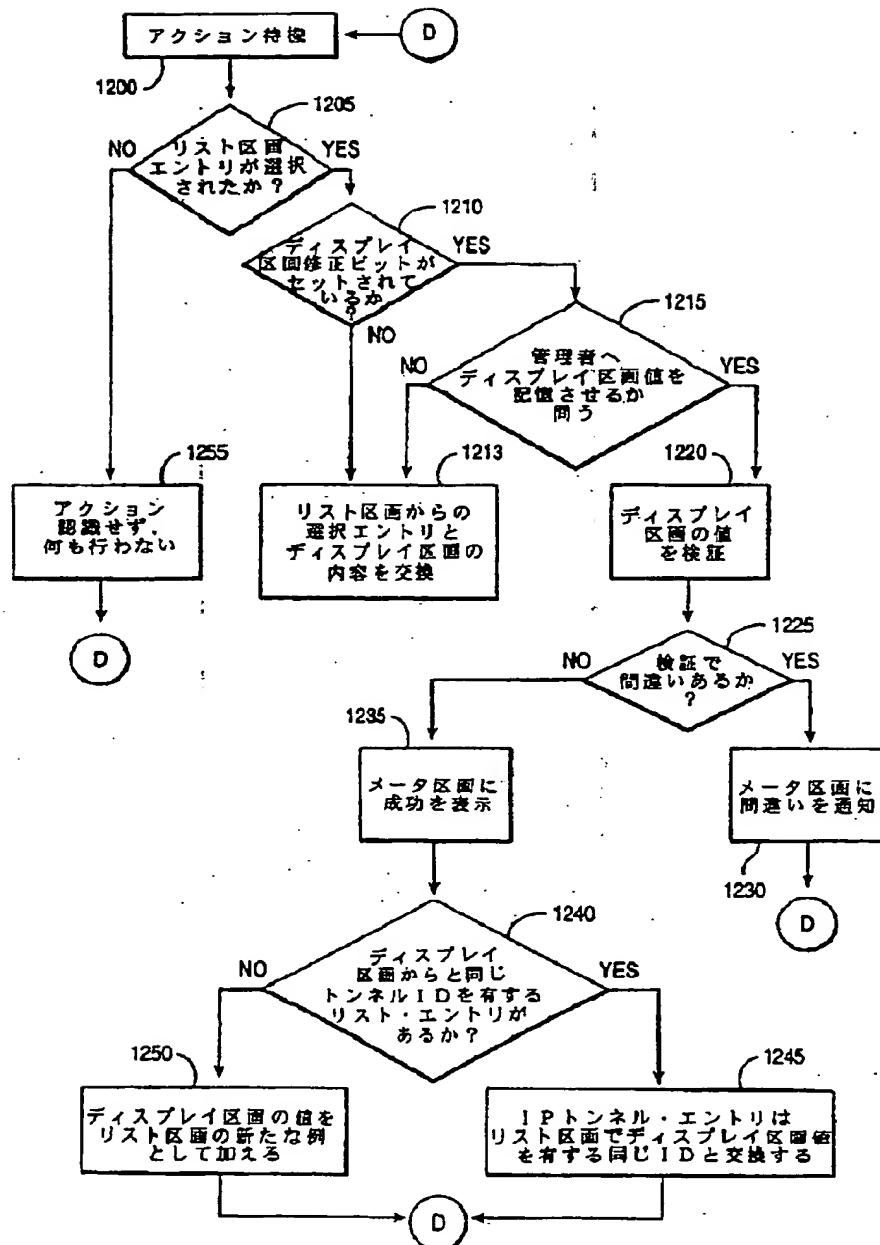
【図8】



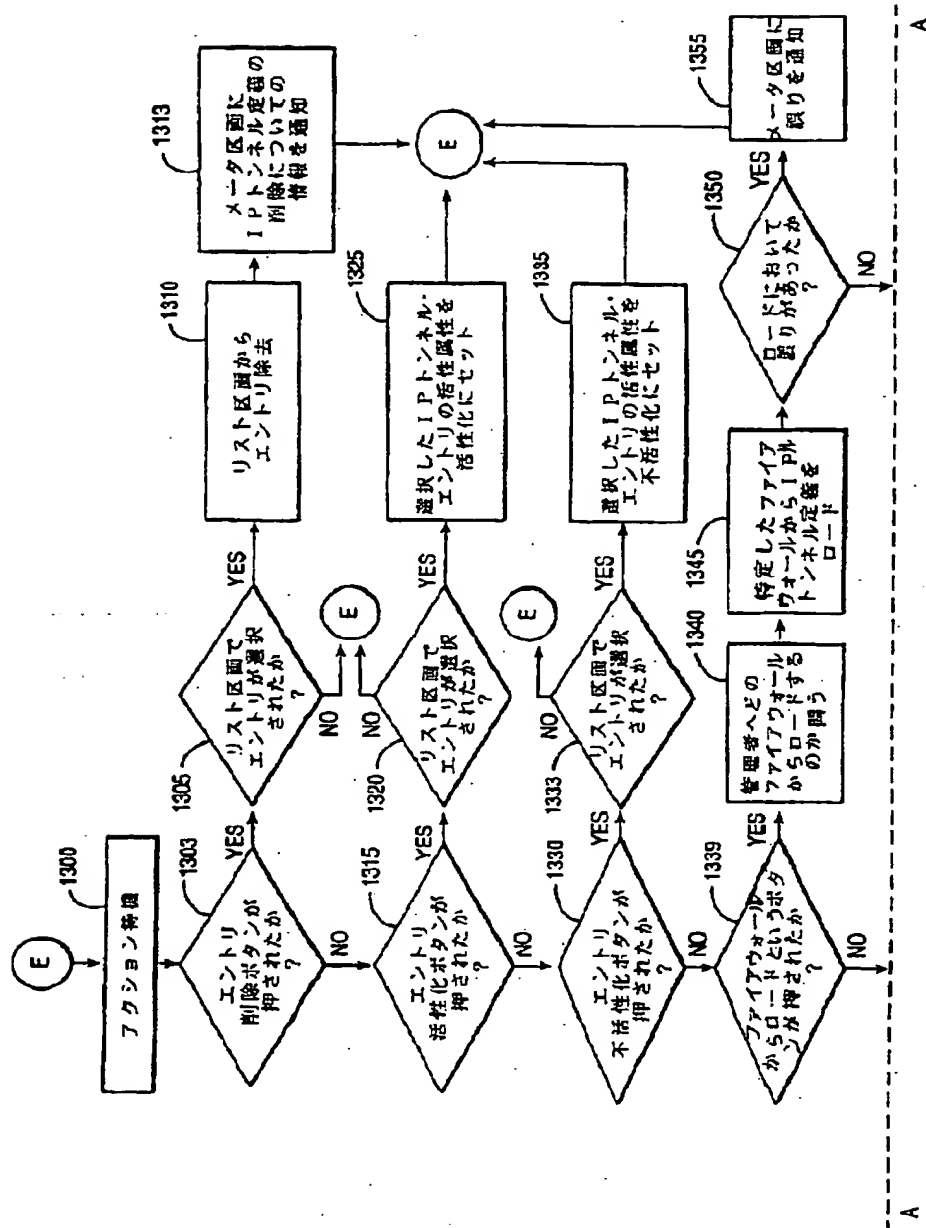
【図9】



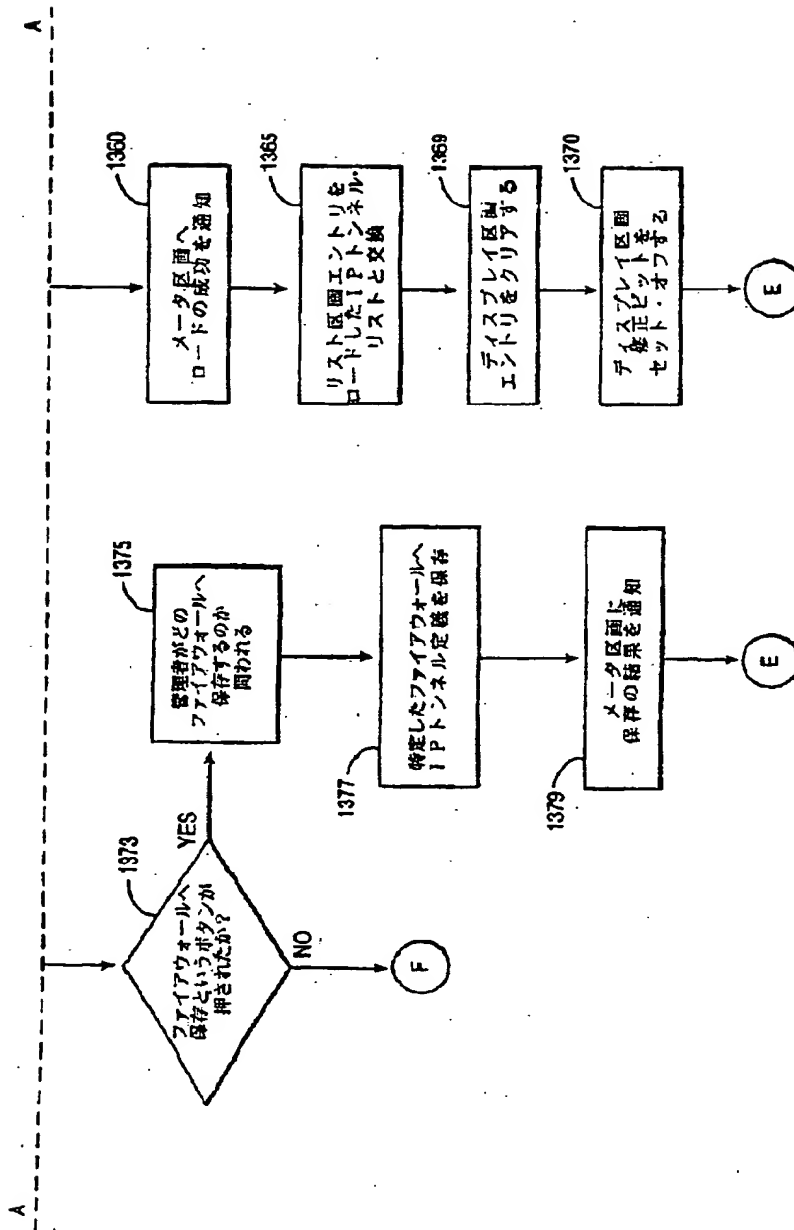
【図10】



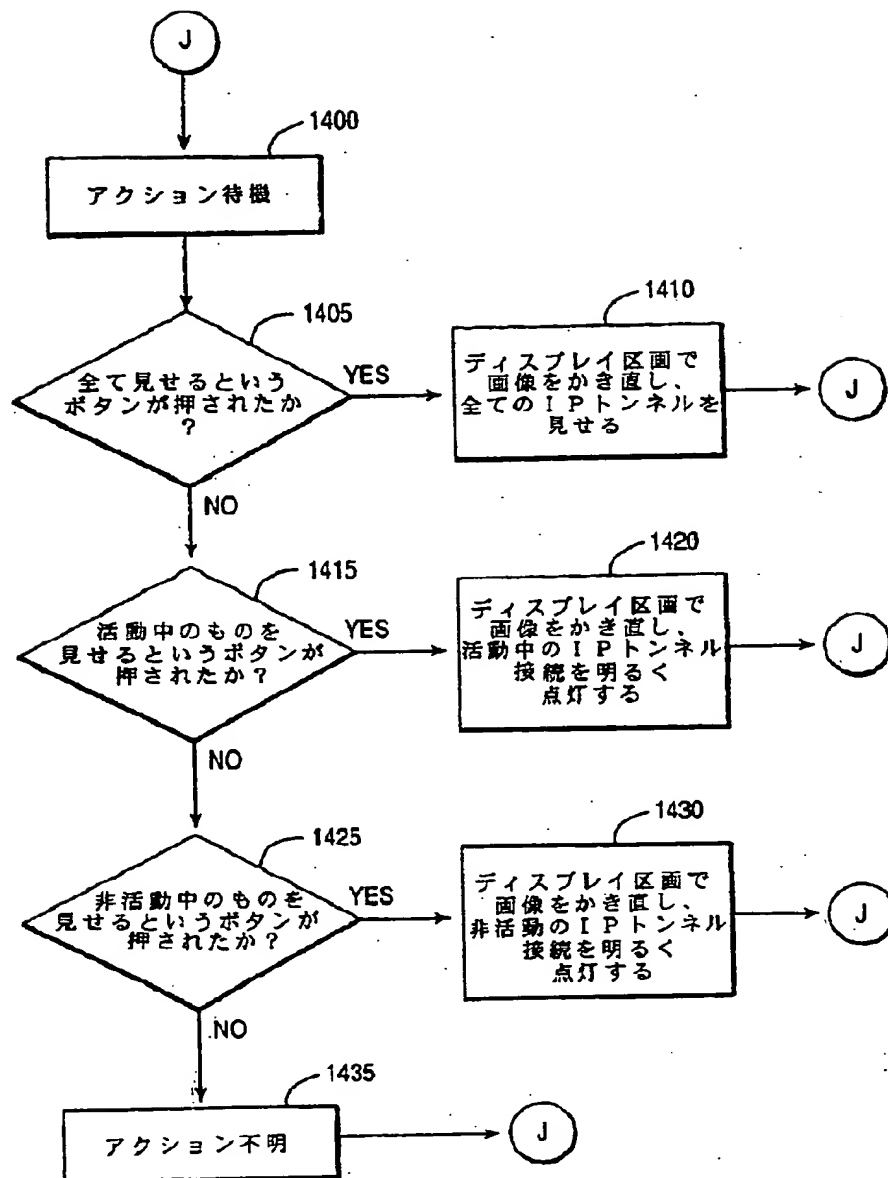
〔図11〕



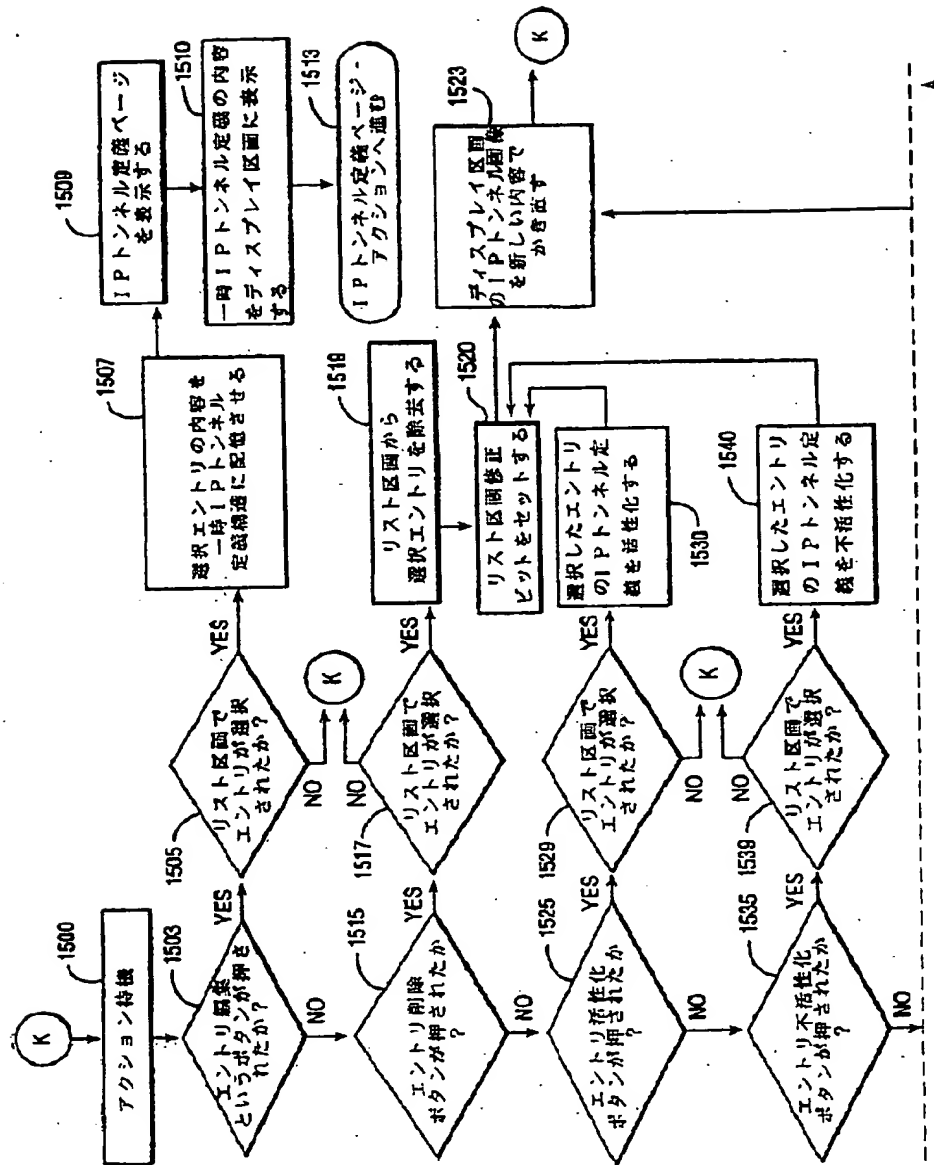
〔図12〕



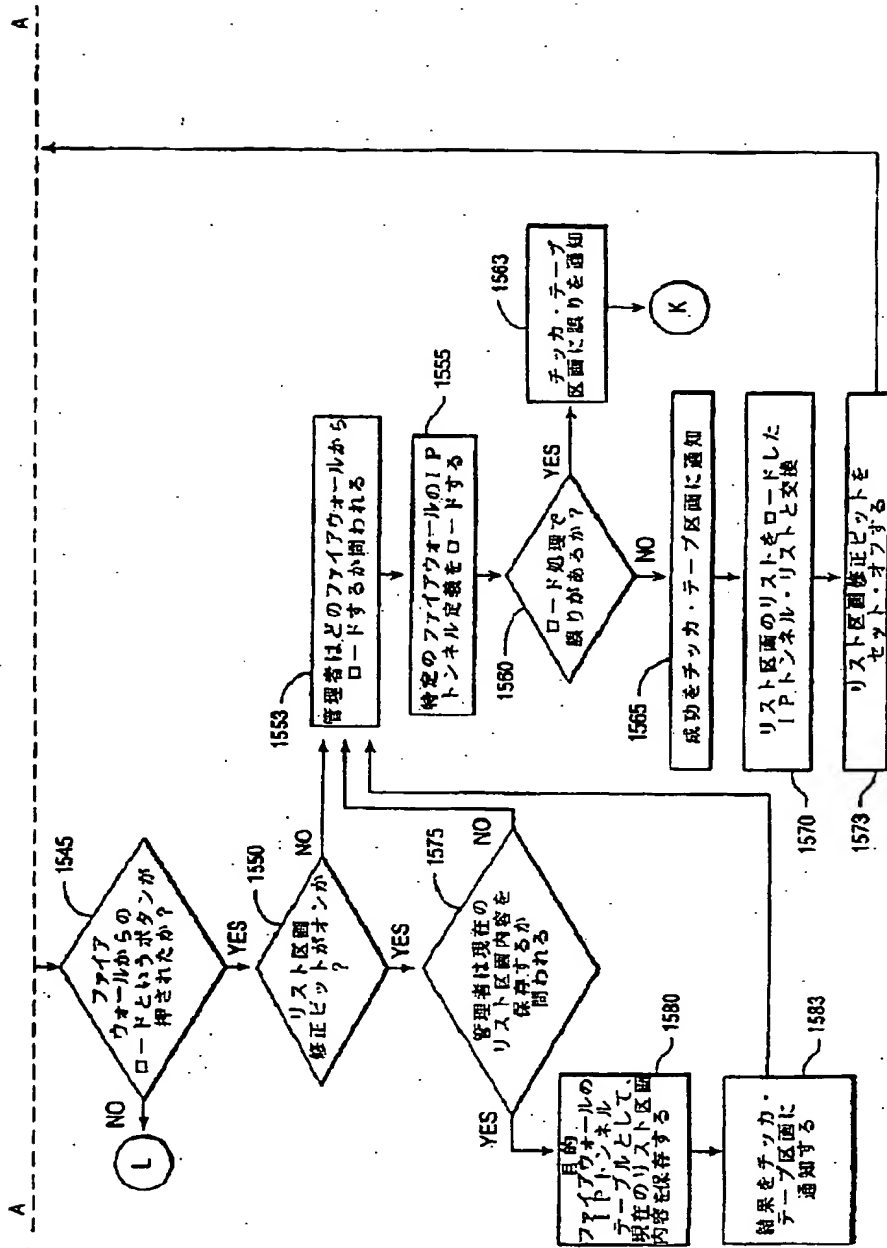
【図14】



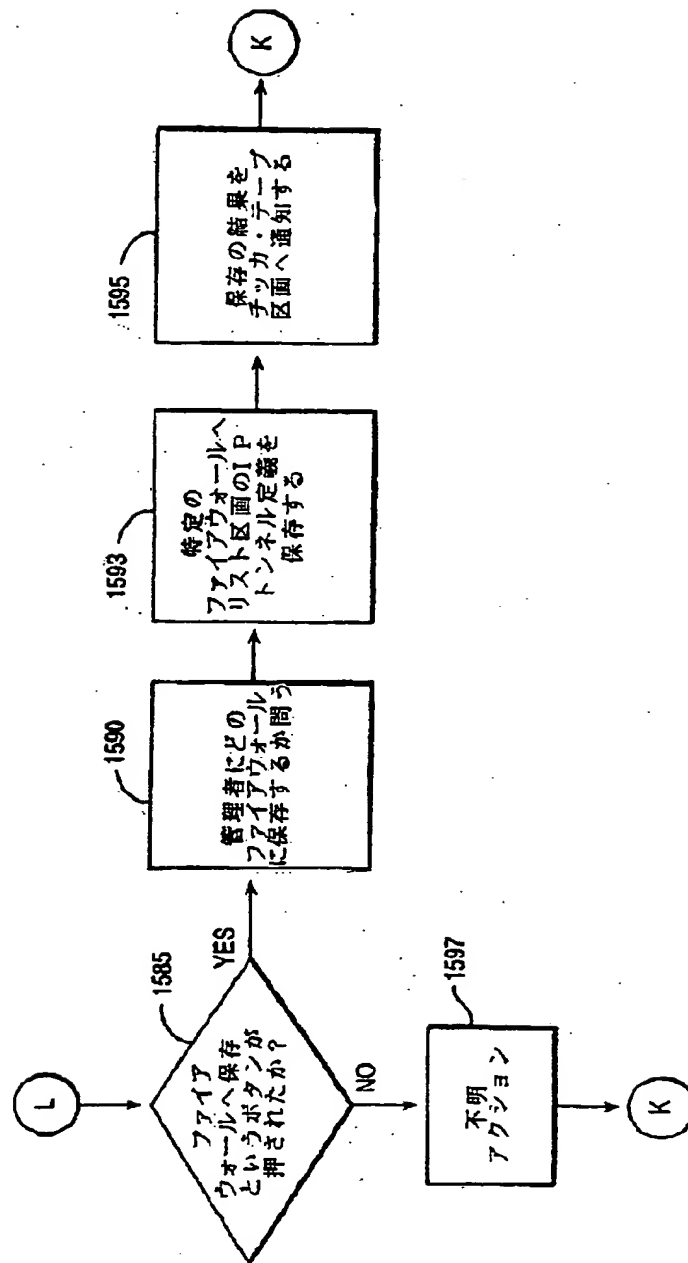
〔図15〕



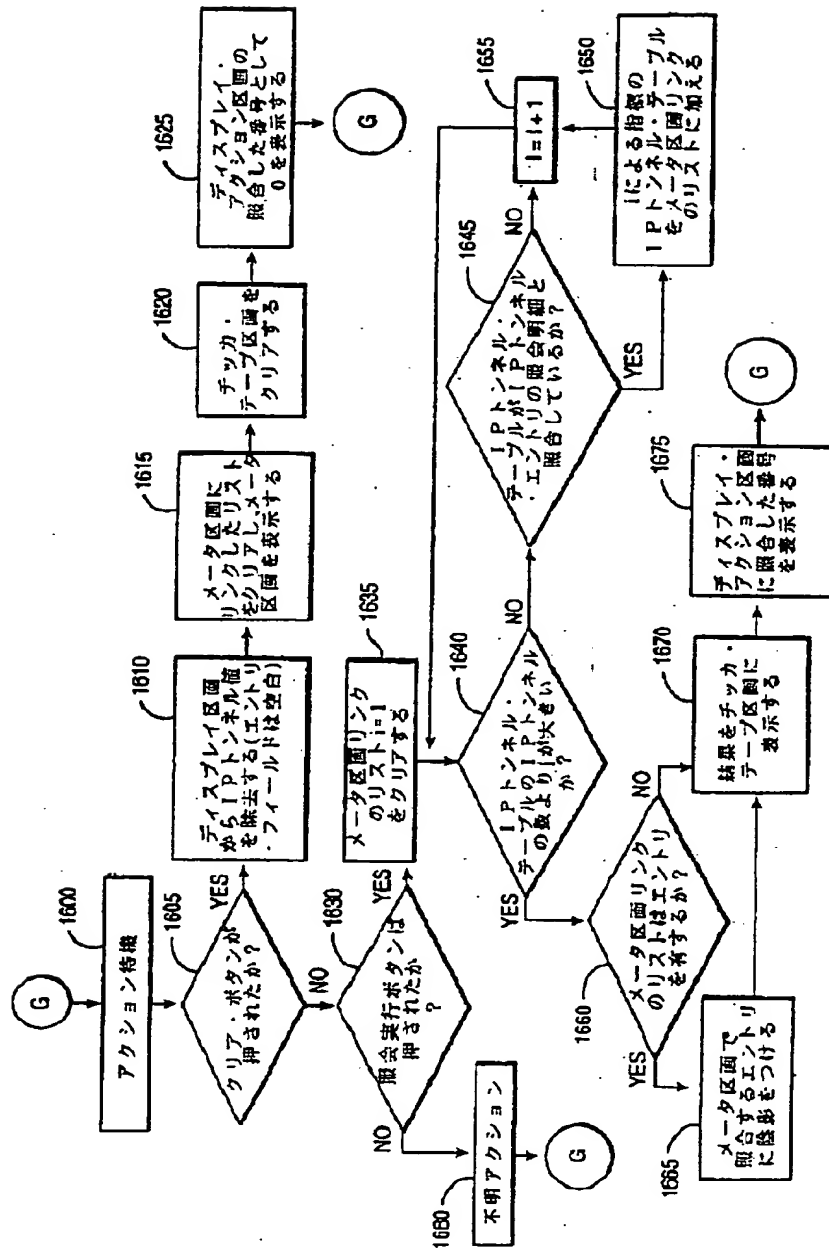
【図16】



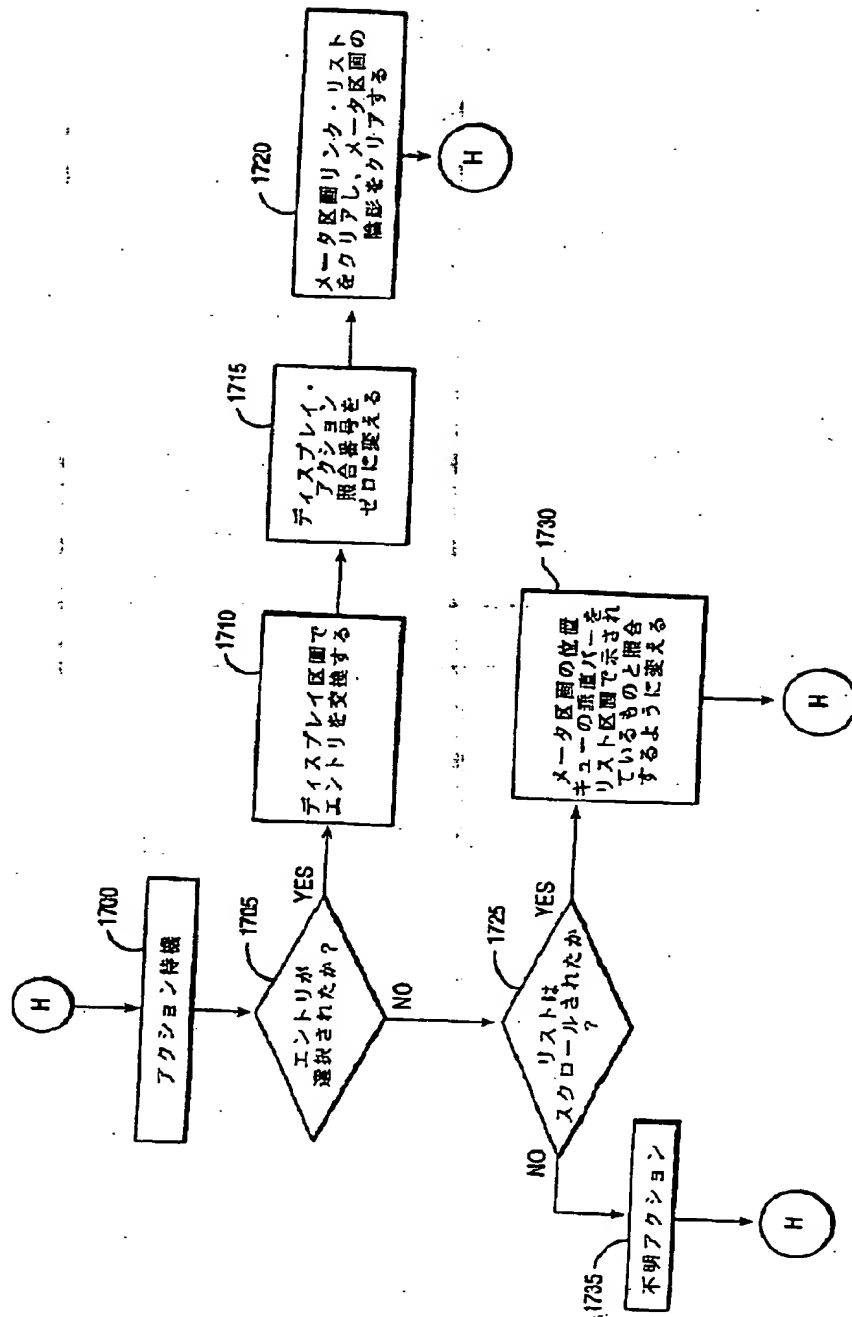
【図17】



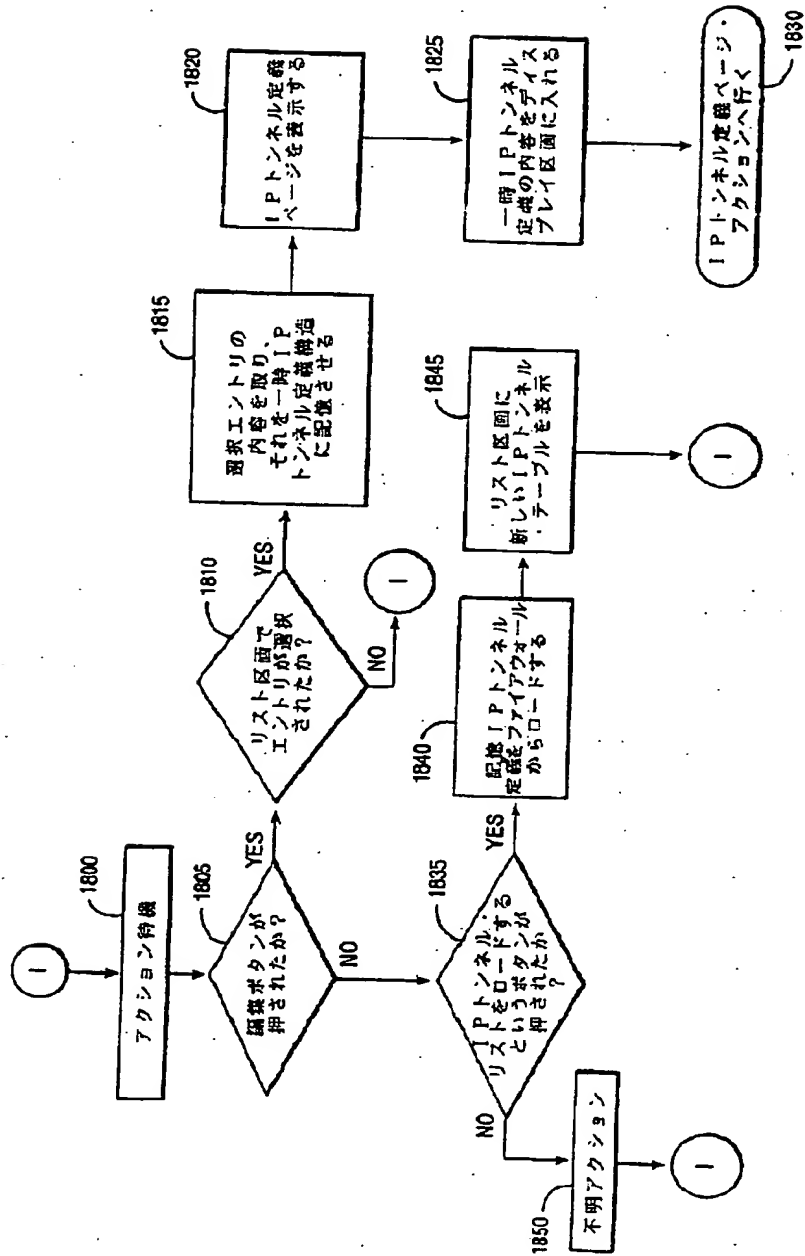
〔図18〕



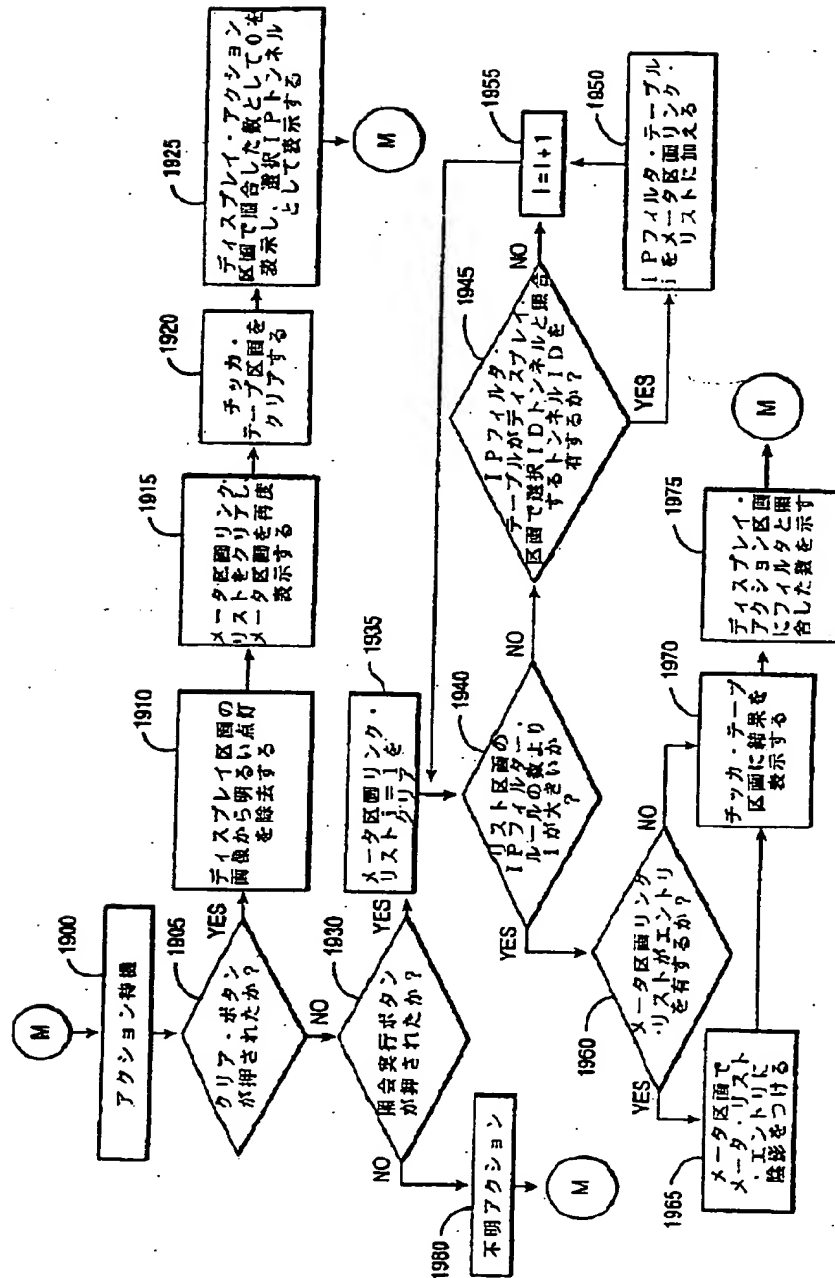
【図19】



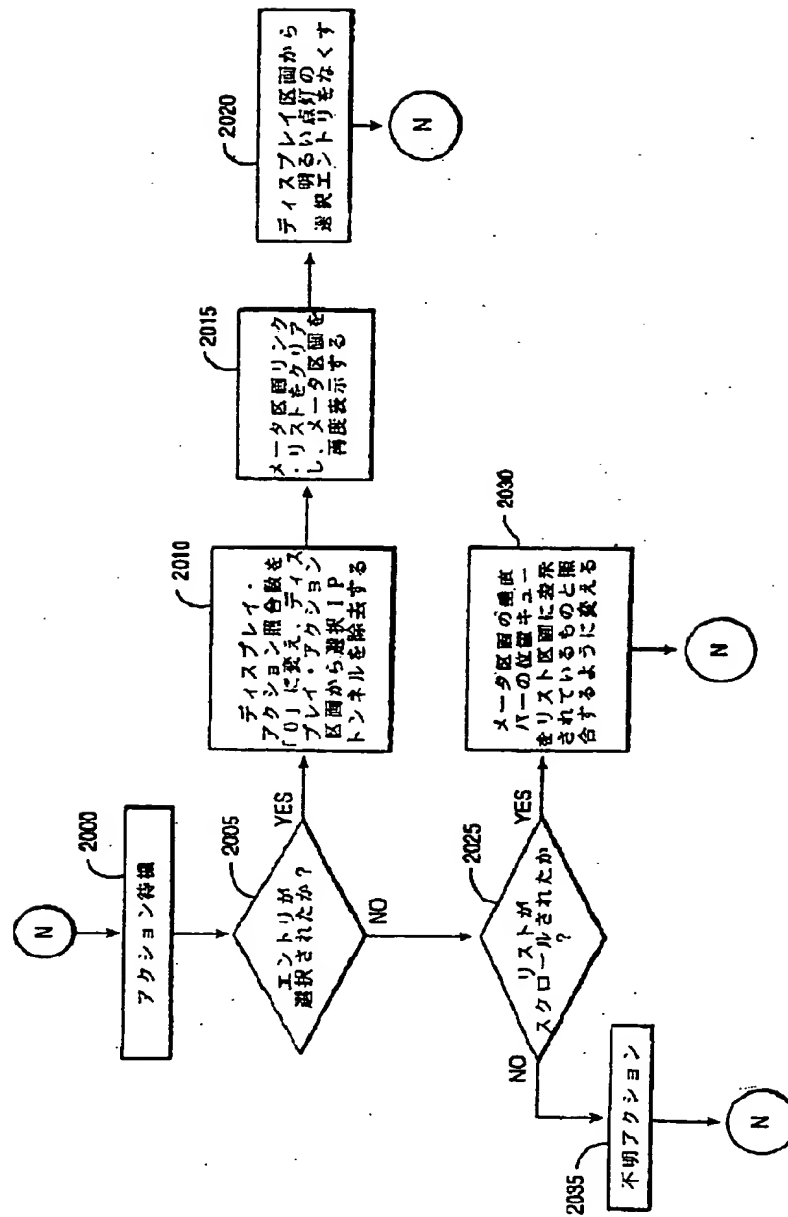
【図20】



〔図21〕



【図22】



【図23】

